目 录

第一章 抽象代数的基本概念和有限域的结构

抽象代数一般被认为是研究代数结构的性质的理论. 在这一章里我们将介绍群、环、域这三个基本代数结构的定义,并详细地讨论有限域的结构. 首先,我们从读者所熟悉的有理数域 $\mathbf{Q}$, 实数域 $\mathbf{R}$ 和复数域 $\mathbf{C}$ 出发归纳出域的概念. 接着我们构造了对于编码理论来说是重要的有限域 $\mathbf{Z}_p$ 和 $\mathbf{Z}_p[x]_{p(x)}$ 作为例子. 我们构造有限域的方法比较形式, 这是因为我们想避免同余类环这一比较复杂的概念, 因而直接在 $\mathbf{Z}_p$ 中引进模 p 加法和模 p 乘法,同时直接在 $\mathbf{Z}_p[x]_{p(x)}$ 中引进模 $p(x)$ 的加法和模 $p(x)$ 的乘法. 对于熟悉模 2 加法的工程技术科研人员来说, 也许这样做并不难接受, 在 § 7 中介绍了同余类环的概念以后,读者也就会更清楚在 $\mathbf{Z}_p$ 和 $\mathbf{Z}_p[x]_{p(x)}$ 中直接引入的加法运算和乘法运算的由来. 在 § 4 里我们从域的加法群和乘法群概括出交换群的概念, 并证明了有限域的乘法群是循环群这一重要结果. § 5 中关于有限域的结构定理, 我们采用的是初等证明, 显得比较复杂. 读者可以从书后所附参考书目中的[11], [13], [14]或[20]里找到用较深工具的简单证明. 为了能概括更广的一些代数结构, 如整数环 $\mathbf{Z}$, 整数模 m 的环 $\mathbf{Z}_m$ (m 是个复合数)以及域上多项式环 $F[x]$, $F[x_1, x_2, \cdots, x_n]$ 等, 我们引进了交换环的概念. 对于了解编码理论的基础部分来说, 一般的群(即它的运算不满足交换律的群) 和一般的环 (即它的乘法运算不满足交换律的环) 并不

十分必要，因此在本书中并没有讨论．对于一般的群和环有兴趣的读者请参考书后所附参考书目中[11]或[12]．为了引进同余类环，同时也为了以后讨论循环码的需要，我们还介绍了理想的概念．在最后一节里我们介绍了我国古代数学的重要成就之一——孙子定理，并着重指出了它与近代环论中环的直和分解的关系．

§1 域的概念

我们从大家都熟悉的有理数开始讨论．我们不是考察一个一个的有理数，而是考察有理数的全体所组成的集合．我们用 $\mathbf{Q}$ 来代表有理数的全体所组成的集合．我们知道，在 $\mathbf{Q}$ 中可以进行四则运算．即任意给了两个有理数 a 和 b，可以对它们进行加法运算，得到它们的和 $a+b$ 也是个有理数；可以对它们进行减法运算，得到它们的差 $a-b$ 也是个有理数；可以对它们进行乘法运算，得到它们的积 $a\cdot b$ 也是个有理数；如果 $b\neq 0$ 的话，还可以用 b 做除数，用 a 做被除数进行除法运算，得到它们的商 $\frac{a}{b}$ 也是个有理数．我们也知道，差可以表成和的形状，即如果用 $-b$ 表示 b 的相反数（适合条件 $b+(-b)=0$ 的数 $-b$），那么 $a-b=a+(-b)$，这样 a 减 b 所得的差就表成了 a 与 $-b$ 的和．同样，商也可以表成积的形状，即当 $b\neq 0$ 时，如果用 b^{-1} 表示 b 的倒数（适合条件 $b\cdot b^{-1}=1$ 的数 b^{-1}），那么 $\frac{a}{b}=a\cdot b^{-1}$，这样 a 被 b 除所得的商就表成了 a 与 b^{-1} 的积．因此在有理数的四则运算中，加法和乘法这两个运算是更为基本的．

我们也都知道，$\mathbf{Q}$ 中的加法和乘法这两种运算满足以下这些运算规则：

I.1　对任意 $a, b\in\mathbf{Q}$, 有

$$a+b=b+a. \quad (\text{加法交换律})$$

I.2　对任意 $a, b, c\in\mathbf{Q}$, 有

$$(a+b)+c=a+(b+c). \quad (\text{加法结合律})$$

I.3　$\mathbf{Q}$ 中有一个数, 即 0, 具有性质

$$a+0=0+a=a, \quad \text{对一切 } a\in\mathbf{Q}.$$

I.4　对任意 $a\in\mathbf{Q}$, $\mathbf{Q}$ 中有一个与它相反的数, 即 $-a$, 具有性质

$$a+(-a)=(-a)+a=0.$$

II.1　对任意 $a, b\in\mathbf{Q}$, 有

$$ab=ba. \quad (\text{乘法交换律})$$

II.2　对任意 $a, b, c\in\mathbf{Q}$, 有

$$(ab)c=a(bc). \quad (\text{乘法结合律})$$

II.3　$\mathbf{Q}$ 中有一个数, 即 1, 具有性质

$$a\cdot 1=1\cdot a=a, \quad \text{对一切 } a\in\mathbf{Q}.$$

II.4　对任意 $a\in\mathbf{Q}$ 而 $a\neq 0$, $\mathbf{Q}$ 中有它的一个倒数, 即 a^{-1}, 具有性质

$$a\cdot a^{-1}=a^{-1}\cdot a=1.$$

III.　对任意 $a, b, c\in\mathbf{Q}$, 有

$$\left.\begin{aligned} a(b+c)&=ab+ac,\\ (b+c)a&=ba+ca. \end{aligned}\right\} \quad (\text{分配律})$$

上面这些运算规则中, I 是关于加法的, II 是关于乘法的, I 和 II 完全是平行的, III 是说乘法对于加法来说是分配的.

我们再考察实数的全体所组成集合, 我们把这个集合记作 $\mathbf{R}$. 我们知道, 在 $\mathbf{R}$ 中也可以进行加法运算和乘法运算: 任意给了两个实数 a 和 b, 对它们进行加法运算, 得到它们的和 $a+b$ 也是个实数; 对它们进行乘法运算, 得到它们的积 $a\cdot b$ 也是个实数. 而且 $\mathbf{R}$ 中加法运算和乘法运算也满足上面

举出的运算规则 I, II, III, 当然要把其中的 $\mathbf{Q}$ 改成 $\mathbf{R}$.

我们再考察复数的全体所组成的集合,并把它记作 $\mathbf{C}$. 在 $\mathbf{C}$ 中也可以进行加法运算和乘法运算: 对于任意 $a, b\in\mathbf{C}$, 它们的和 $a+b$ 与积 $a\cdot b$ 也都是复数,而且 $\mathbf{C}$ 中的加法运算和乘法运算也满足上面举出的运算规则 I, II, III, 当然要把其中的 $\mathbf{Q}$ 改成 $\mathbf{C}$.

从上面这些例子,我们可以归纳出"域"的概念.

定义 1 设 F 是一个非空集合, F 的成员叫做元素. 假定在 F 中规定了加法和乘法这两种运算,即对于 F 中任意两个元素 a 和 b, 可以对它们进行*加法运算和乘法运算*,把加法运算的结果记作 $a+b$, 叫做它们的*和*, 并把乘法运算的结果记作 $a\cdot b$, 叫做它们的*积*. 我们还要求 F 中任意两个元素经加法运算和乘法运算的结果仍是 F 中的元素,即 F 中任意两个元素的和与积仍都是 F 中的元素(这个性质通常称为 F 对于加法运算和乘法运算是*自封的*). 我们说 F 对于所规定的加法运算和乘法运算是一个*域*,如果以下运算规则都成立:

I.1 对任意 $a, b\in F$, 有

$$a+b=b+a;$$

I.2 对任意 $a, b, c\in F$, 有

$$(a+b)+c=a+(b+c);$$

I.3 F 中有一个元素,把它记作 0, 具有性质

$$a+0=a, \quad \text{对一切 } a\in F;$$

I.4 对任意 $a\in F$, F 中有一个元素, 把它记作 $-a$, 具有性质

$$a+(-a)=0;$$

II.1 对任意 $a, b\in F$,有

$$a\cdot b=b\cdot a;$$

II.2 对任意 $a, b, c\in F$, 有

$$(a\cdot b)\cdot c=a\cdot(b\cdot c);$$

II.3　F 中有一个 $\neq 0$ 的元素，把它记作 e，具有性质

$$a\cdot e=a,\ \text{对一切}\ a\in F;$$

II.4　对任意 $a\in F$ 而 $a\neq 0$，F 中有一个元素，把它记作 a^{-1}，具有性质

$$a\cdot a^{-1}=e;$$

III　对任意 $a, b, c\in F$，有

$$a\cdot(b+c)=a\cdot b+a\cdot c.$$

值得注意的是，在这个定义里，因为假设了加法交换律 I.1 成立，所以在 I.3 中我们仅仅要求 $a+0=a$，而略去了 $0+a=a$ 这一要求，这是由于从 I.1 和 $a+0=a$ 可以推出 $0+a=a$；同理，我们在 I.4 中只要求 $a+(-a)=0$，而略去了 $(-a)+a=0$ 这一要求．因为我们在这个定义里假设了乘法交换律 II.1 成立，所以在 II.3 中只要求 $a\cdot e=a$，而略去了 $e\cdot a=a$ 这一要求；在 II.4 中只要求 $a\cdot a^{-1}=e$，而略去 $a^{-1}\cdot a=e$ 这一要求；在 III 中也略去了 $(b+c)\cdot a=b\cdot a+c\cdot a$ 这一要求．

基于这个定义并根据前面的分析，我们可以说，所有有理数组成的集合 $\mathbf{Q}$ 对于有理数的加法和乘法运算来说是一个域，叫做*有理数域*；所有实数组成的集合 $\mathbf{R}$ 对于实数的加法和乘法运算来说是一个域，叫做*实数域*；所有复数组成的集合 $\mathbf{C}$ 对于复数的加法和乘法运算来说也是一个域，叫做*复数域*．我们也知道 $\mathbf{R}$ 是 $\mathbf{C}$ 的子集，而 $\mathbf{R}$ 中的加法运算和乘法运算即是把 $\mathbf{R}$ 中的元素看作 $\mathbf{C}$ 中元素所作的加法运算和乘法运算．这时我们说 $\mathbf{R}$ 是 $\mathbf{C}$ 的*子域*．一般地，我们有下面这个定义．

定义 2　设 F 是一个域，而 F_0 是 F 的一个非空子集．如果 F_0 对于 F 中的加法运算和乘法运算来说是一个域，这就是说，对 F_0 中任意两个元素按 F 中加法运算和乘法运算进行运

算所得的和与积仍是F_0中的元素，而且F中的加法运算和乘法运算对于F_0来说也满足定义1中的运算规则I, II, III，我们就说F_0是F的子域.

值得注意的是，设F是域，而F_0是F的一个非空子集，如果F_0对于F中的加法运算和乘法运算自封，那么要验证F_0是F的子域，只要验证I.3, I.4, II.3, II.4在F_0中成立就行了，因为这时I.1, I.2, II.1, II.2, III在F_0中自然成立.

根据定义2，我们可以说$\mathbf{R}$是$\mathbf{C}$的子域，$\mathbf{Q}$也是$\mathbf{C}$的子域，$\mathbf{Q}$还是$\mathbf{R}$的子域.

为了搞清楚域的概念，下面我们再举几个例子.

例1 考察所有形状

$$a+b\sqrt{2}, \quad a, b\in\mathbf{Q}$$

的实数的全体所组成的集合，把这个集合记作$\mathbf{Q}[\sqrt{2}]$. 我们规定$\mathbf{Q}[\sqrt{2}]$中两个元素的和与积分别是它们作为实数的和与积. 我们来验证$\mathbf{Q}[\sqrt{2}]$对于实数的加法运算和乘法运算是一个域，因而是$\mathbf{R}$的子域. 首先，设$a+b\sqrt{2}$, $c+d\sqrt{2}\in\mathbf{Q}[\sqrt{2}]$，那么

$$\begin{aligned}&(a+b\sqrt{2})+(c+d\sqrt{2})\\=&(a+c)+(b+d)\sqrt{2},\\&(a+b\sqrt{2})\cdot(c+d\sqrt{2})\\=&(ac+2bd)+(ad+bc)\sqrt{2}.\end{aligned}$$

显然$a+c$, $b+d$, $ac+2bd$, $ad+bc\in\mathbf{Q}$. 因此$\mathbf{Q}[\sqrt{2}]$对于加法运算和乘法运算是自封的，其次，还要验证$\mathbf{Q}[\sqrt{2}]$中的加法运算和乘法运算满足运算规则I.3, I.4, II.3, II.4.

显然 $0=0+0\sqrt{2}\in\mathbf{Q}[\sqrt{2}]$，而对一切$a+b\sqrt{2}\in\mathbf{Q}[\sqrt{2}]$，有$(a+b\sqrt{2})+0=a+b\sqrt{2}$. 因此I.3成立. 其次，对任意$a+b\sqrt{2}\in\mathbf{Q}[\sqrt{2}]$，有$-a+(-b)\sqrt{2}\in\mathbf{Q}[\sqrt{2}]$，而

$$(a+b\sqrt{2})+[-a+(-b)\sqrt{2}]=0,$$

因此 I.4 也成立.

可以平行地证明 II.3 和 II.4 也成立，只要注意 $1=1+0\sqrt{2}\in\mathbf{Q}[\sqrt{2}]$；而当 $a+b\sqrt{2}\in\mathbf{Q}[\sqrt{2}]$，$a+b\sqrt{2}\neq 0$ 时，$a^2-2b^2\neq 0$，因此

$$\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in\mathbf{Q}[\sqrt{2}],$$

而且 $$(a+b\sqrt{2})\cdot\left(\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\right)=1.$$

这证明了 $\mathbf{Q}[\sqrt{2}]$ 是 $\mathbf{R}$ 的子域.

例 2 考察所有形状

$$a+b\sqrt[3]{2},\quad a,\ b\in\mathbf{Q}$$

的实数的全体所组成的集合，并把这个集合记作 S. 如果规定 S 中两个元素的和与积分别是它们作为实数的和与积，这时 S 不是域，这是因为 S 对于乘法运算不是自封的. 例如

$$\sqrt[3]{2}\cdot\sqrt[3]{2}=\sqrt[3]{4}$$

就不是形状 $a+b\sqrt[3]{2}$ $(a,\ b\in\mathbf{Q})$ 的数.

但是，如果考察所有形状

$$a+b\sqrt[3]{2}+c\sqrt[3]{4},\qquad a,\ b,\ c\in\mathbf{Q}$$

的实数的集合，把这个集合记作 $\mathbf{Q}[\sqrt[3]{2}]$，并规定 $\mathbf{Q}[\sqrt[3]{2}]$ 中两个元素的和与积分别是它们作为实数的和与积，可以验证 $\mathbf{Q}[\sqrt[3]{2}]$ 是域. 请读者自己验证一下.

例 3 考察全体整数(正、负整数和 0)的集合，并把这个集合记作 $\mathbf{Z}$. 固然 $\mathbf{Z}$ 对于整数的加法运算和乘法运算是自封的，而且 $\mathbf{Z}$ 中加法运算和乘法运算满足运算规则 I.1, I.2, I.3, I.4, II.1, II.2, II.3 和 III，但是在 $\mathbf{Z}$ 中 II.4，却不成立. 譬如，2 和任意整数之积都不能等于 1. 因此 $\mathbf{Z}$ 不是域.

下面我们经常要用到关于整数分解的一些性质. 不熟悉

这部分内容的读者请先阅读本书的附录二.

无论是$\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$或是$\mathbf{Q}[\sqrt{2}]$, $\mathbf{Q}[\sqrt[3]{2}]$,它们的元素个数都是无限的. 但在编码里用的却是元素个数有限的域. 我们有

定义 3 设F是域. 如果F的元素个数无限,F就叫无限域. 如果F的元素个数有限,F就叫有限域也叫伽罗瓦(Galois)域.

我们举一个有限域的例子.

例 4 设p是一个给定的素数. 令$\mathbf{Z}_p$表示所有$<p$的非负整数所组成的集合

$$\mathbf{Z}_p=\{0, 1, 2, \cdots, p-1\}.$$

显然按照通常的整数加法运算和乘法运算,$\mathbf{Z}_p$不是域,因为$\mathbf{Z}_p$对于通常的整数加法运算和乘法运算都不自封. 下面我们将用另外的方法来规定$\mathbf{Z}_p$中的加法和乘法运算使$\mathbf{Z}_p$成域.

我们先引进一个记号,这个记号今后经常要用到. 设a和b是两个整数,而$b\neq 0$. 再设用b去除a所得的商是q而余数是r,即

$$a=qb+r, \quad 0\leqslant r<|b|.$$

我们知道,q和r由a和b唯一确定. 引进记号

$$r=(a)_b$$

来表示用b去除a所得的余数.

现在设a, $b\in\mathbf{Z}_p$. 我们按下式来规定a与b的和(把它记作$a\oplus b$)与积(把它记作$a\odot b$):

$$a\oplus b=(a+b)_p,$$
$$a\odot b=(a\cdot b)_p.$$

我们也常把$\mathbf{Z}_p$中的加法$\oplus$叫做模p加法,而把$\mathbf{Z}_p$中的乘法$\odot$叫做模p乘法. 我们来验证$\mathbf{Z}_p$对于如上规定的加法和乘

法运算是域.

首先,显然有

$$0\leqslant(a+b)_p<p,\quad 0\leqslant(a\cdot b)_p<p.$$

因此 $\mathbf{Z}_p$ 对于模 p 加法和模 p 乘法是自封的.

其次要验证如上规定的 $\mathbf{Z}_p$ 中的模 p 加法和模 p 乘法满足运算规则 I, II, III.

先证 I.1 和 II.1 成立. 对任意 $a, b\in\mathbf{Z}_p$, 我们有

$$a+b=b+a,\quad ab=ba.$$

因此 $$(a+b)_p=(b+a)_p,\quad (a\cdot b)_p=(b\cdot a)_p.$$

这就是说 $$a\oplus b=b\oplus a,\quad a\odot b=b\odot a.$$

在验证 I.2 和 II.2 之前,我们先证明下面这个引理.

引理 1 设 a_1, a_2, b 都是整数, 而 $b\neq 0$. 那么 $(a_1)_b=(a_2)_b$, 当且仅当 $b|a_1-a_2$*.

证. “$(a_1)_b=(a_2)_b$, 当且仅当 $b|a_1-a_2$” 这个命题的涵意是说“当 $b|a_1-a_2$ 时, $(a_1)_b=(a_2)_b$”及“当 $(a_1)_b=(a_2)_b$时, $b|a_1-a_2$”这两个命题同时成立.

根据带余除法,可以设

$$a_1=q_1b+(a_1)_b,\quad 0\leqslant(a_1)_b<|b|.$$
$$a_2=q_2b+(a_2)_b,\quad 0\leqslant(a_2)_b<|b|.$$

那么

$$a_1-a_2=(q_1-q_2)b+(a_1)_b-(a_2)_b. \tag{1}$$

当 $b|a_1-a_2$时,由(1)式可推出 $b|(a_1)_b-(a_2)_b$. 但因 $0\leqslant(a_1)_b, (a_2)_b<|b|$, 故 $0\leqslant|(a_1)_b-(a_2)_b|<|b|$. 因此一定有 $(a_1)_b=(a_2)_b$. 反过来,当 $(a_1)_b=(a_2)_b$ 时, 由(1)式显然有 $b|a_1-a_2$. 这就证明了引理 1.

从引理 1 可以推出关于符号 $(a)_b$ 的运算规则,即

引理 2 设 a_1, a_2, b 都是整数,而 $b\neq 0$, 那么

---

* $b|a$ 表示 a 能被 b 整除.

$$(a_1 \pm a_2)_b = ((a_1)_b \pm (a_2)_b)_b, \tag{2}$$

$$(a_1 a_2)_b = ((a_1)_b \cdot (a_2)_b)_b. \tag{3}$$

((2)式实际是两个式子,等号双方取'+'号得到一个式子,等号双方取'－'号又得到一个式子. 以后出现符号'±'时,也作此了解,而不一一说明.)

证. 首先注意,对于任意整数 a, 根据带余除法, 可以写

$$a = qb + (a)_b, \quad 0 \leqslant (a)_b < |b|.$$

因此 $$b \mid a - (a)_b.$$

特别,因

$$(a_1 \pm a_2) - ((a_1)_b \pm (a_2)_b) = (a_1 - (a_1)_b) \pm (a_2 - (a_2)_b)$$

和 $$a_1 a_2 - (a_1)_b (a_2)_b = a_1 (a_2 - (a_2)_b) + (a_1 - (a_1)_b)(a_2)_b$$

都是 b 的倍数,所以根据引理 1 就推出(2), (3)两式.

显然, 可以将引理 2 推广到 n 个整数 $a_i (i=1, 2, \cdots, n)$ 的和与积的情形,即

$$(a_1 + a_2 + \cdots + a_n)_b = ((a_1)_b + (a_2)_b + \cdots + (a_n)_b)_b,$$

$$(a_1 a_2 \cdots a_n)_b = ((a_1)_b \cdot (a_2)_b \cdots (a_n)_b)_b.$$

请读者自己把证明补出.

现在来验证在 $\mathbf{Z}_p$ 中 I.2 和 II.2 成立. 由 $\mathbf{Z}_p$ 中加法运算和乘法运算的定义可知,对任意 $a, b, c \in \mathbf{Z}_p$, 有

$$(a \oplus b) \oplus c = ((a+b)_p + c)_p,$$

$$(a \odot b) \odot c = ((ab)_p \cdot c)_p.$$

因 $c \in \mathbf{Z}_p$, 所以 $(c)_p = c$. 因此由引理 2 推出

$$((a+b)_p + c)_p = ((a+b) + c)_p,$$

$$((ab)_p \cdot c)_p = ((ab)c)_p.$$

再根据整数加法和乘法的结合律可知

$$(a+b) + c = a + (b+c),$$

$$(ab) \cdot c = a \cdot (bc).$$

因此 $$((a+b)+c)_p = (a + (b+c))_p,$$

$$((ab)\cdot c)_p=(a\cdot(bc))_p.$$

仍根据引理 2，有

$$(a+(b+c))_p=(a+(b+c)_p)_p,$$

$$(a\cdot(bc))_p=(a\cdot(bc)_p)_p.$$

再根据 $\mathbf{Z}_p$ 中模 p 加法和模 p 乘法的定义有

$$(a+(b+c)_p)_p=a\oplus(b\oplus c),$$

$$(a\cdot(bc)_p)_p=a\odot(b\odot c).$$

那么从以上诸式立刻推出

$$(a\oplus b)\oplus c=a\oplus(b\oplus c),$$

$$(a\odot b)\odot c=a\odot(b\odot c).$$

这证明了 I.2 和 II.2 在 $\mathbf{Z}_p$ 中都成立.

先来验证 III 在 $\mathbf{Z}_p$ 中成立. 根据 $\mathbf{Z}_p$ 中加法运算和乘法运算的定义有

$$a\odot(b\oplus c)=(a\cdot(b+c)_p)_p.$$

根据引理2，有

$$(a\cdot(b+c)_p)_p=(a\cdot(b+c))_p.$$

因为整数的乘法运算对于加法运算是分配的，有

$$a\cdot(b+c)=ab+ac.$$

因而有 $$(a\cdot(b+c))_p=(ab+ac)_p.$$

仍根据引理 2，有

$$(ab+ac)_p=((ab)_p+(ac)_p)_p$$

再根据 $\mathbf{Z}_p$ 中加法运算和乘法运算的定义，有

$$((ab)_p+(ac)_p)_p=a\odot b\oplus a\odot c.$$

那么从以上诸式推出

$$a\odot(b\oplus c)=a\odot b\oplus a\odot c.$$

这证明了 III 在 $\mathbf{Z}_p$ 中成立.

再来证明在 $\mathbf{Z}_p$ 中 I.3 和 II.3 成立. 显然对任意 $a\in\mathbf{Z}_p$，有

$$a+0=a.$$

因此 $a \oplus 0=(a+0)_p=(a)_p=a,\quad$ 对任意 $a\in \mathbf{Z}_p$.

这表明 $\mathbf{Z}_p$ 中 0 这个元素有 I.3 所要求的性质. 可以平行地证明 $\mathbf{Z}_p$ 中 1 这个元素有 II.3 所要求的性质, 即

$$a \odot 1=a,\quad \text{对任意 } a\in \mathbf{Z}_p.$$

再来证明在 $\mathbf{Z}_p$ 中 I.4 成立. 对于任意 $a\in \mathbf{Z}_p$, 即 $0\leqslant a<p$, 一定有 $(p-a)_p\in \mathbf{Z}_p$. 显然有

$$a\oplus (p-a)_p=(a+(p-a)_p)_p=(p)_p=0.$$

这表明对于任一给定的 $a\in \mathbf{Z}_p$, $\mathbf{Z}_p$ 中 $(p-a)_p$ 这个元素有 I.4 所要求的性质.

最后来证明 $\mathbf{Z}_p$ 中 II.4 成立. 对任意 $a\in \mathbf{Z}_p$ 而 $a\neq 0$, 即 $0<a<p$, 因 p 是素数, 所以 (a, p)* $=1$. 那么一定有整数 c 和 d 存在使

$$1=ca+dp.$$

显然 $p\,|\,(ca+dp)-ca$. 因此根据引理 1, 有

$$1=(1)_p=(ca+dp)_p=(ca)_p$$

根据带余除法, 可设

$$c=qp+(c)_p,\ 0\leqslant (c)_p<p.$$

仍根据引理 1, 有

$$\begin{aligned}1&=(ca)_p=((qp+(c)_p)a)_p=(qpa+(c)_pa)_p\\&=((c)_p\cdot a)_p=(a\cdot (c)_p)_p.\end{aligned}$$

再根据 $\mathbf{Z}_p$ 中乘法运算的定义, 有

$$(a\cdot (c)_p)_p=a\odot (c)_p.$$

因此 $$1=a\odot (c)_p.$$

这表明 $\mathbf{Z}_p$ 中的元素 $(c)_p$ 有 II.4 所要求的性质.

这证明了 $\mathbf{Z}_p$ 是一个域.

$\mathbf{Z}_p$ 正好有 p 个元素, 因此是个有限域. 因为素数的个数是无限的, 而对任一素数, 我们都如上定义了一个有限域, 所

* (a, b) 表示 a 与 b 两个整数的最大公因数.

以我们得到了无限多个有限域.

特别，当 $p=2$ 时，我们得到一个仅含两个元素 0 和 1 的有限域 $\mathbf{Z}_2$. 它的加法表和乘法表分别是

⊗	0	1
0	0	1
1	1	0

⊙	0	1
0	0	0
1	0	1

加法表的读法是: 加号⊕下面的 $a(=0$ 或 $1)$ 与加号⊕右侧的 $b(=0$ 或 $1)$ 相加所得的和 $a+b$ 是 a 所在的行与 b 所在列的公共元素. 因此有

$$0+0=0,\quad 0+1=1,\quad 1+0=1,\quad 1+1=0.$$

乘法表的读法是: 乘号⊙下面的 $a(=0$ 或 $1)$ 与乘号⊙右侧的 $b(=0$ 或 $1)$ 相乘所得的积 $a\cdot b$ 是 a 所在的行与 b 所在的列的公共元素. 于是有

$$0\cdot 0=0,\quad 0\cdot 1=0,\quad 1\cdot 0=0,\quad 1\cdot 1=1.$$

值得注意的是，在 $\mathbf{Z}_2$ 中，

$$1\oplus 1=0.$$

当 $p=3$ 时，我们得到一个含 3 个元素 0, 1 和 2 的有限域 $\mathbf{Z}_3$. 它的加法表和乘法表分别是

⊕	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

⊙	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

在 $\mathbf{Z}_3$ 中，
$$1\oplus1\oplus1=0$$

一般地，在 $\mathbf{Z}_p$ 中，

$$\underbrace{1\oplus1\oplus\cdots\oplus1}_{p\text{个}1}=(\underbrace{1+1+\cdots+1}_{p\text{个}1})_p=(p)_p=0.$$

这一点与 $\mathbf{Q}$, $\mathbf{R}$ 以及 $\mathbf{C}$ 中的加法很不一样.

一个自然发生的问题是：如果在上面的讨论中用一个复合数（既不是 1 也不是素数的正整数叫复合数）m 来代替素数 p，即令

$$\mathbf{Z}_m=\{0,\ 1,\ 2,\ \cdots,\ m-1\}$$

并按同样方法来规定 $\mathbf{Z}_m$ 中的加法运算和乘法运算，即如果 $a,\ b\in\mathbf{Z}_m$，规定

$$a\oplus b=(a+b)_m,$$
$$a\odot b=(a\cdot b)_m,$$

并把它们分别称为模 m 加法和模 m 乘法．我们问这时 $\mathbf{Z}_m$ 是不是域？仔细检查一下上面的证明可以看出 $\mathbf{Z}_m$ 对于如上规定的加法运算和乘法运算都是自封的，而且上面关于 I, II.1, II.2, II.3 和 III 在 $\mathbf{Z}_p$ 中成立的验证可以原封不动地搬到 $\mathbf{Z}_m$ 上来．但是在 $\mathbf{Z}_m$ 中，II.4 却不成立．实际上，因 m 是复合数，m 就有一个真因数分解

$$m=m_1m_2,\quad 1<m_1,\quad m_2<m.$$

因此 $m_1,\ m_2\in\mathbf{Z}_m$．于是

$$m_1\odot m_2=(m_1\cdot m_2)_m=(m)_m=0.$$

显然 $m_2\neq0$，但对于 m_2 不可能有 $m_2^{-1}\in\mathbf{Z}_m$ 使 $m_2\odot m_2^{-1}=1$；因为否则将有

$$\begin{aligned}m_1=m_1\odot1&=m_1\odot(m_2\odot m_2^{-1})\\&=(m_1\odot m_2)\odot m_2^{-1}=0\odot m_2^{-1}=0,\end{aligned}$$

这与 $1<m_1<m$ 相矛盾．因此，当 m 是复合数时，$\mathbf{Z}_m$ 不是域．

我们往往把定义 1 中的 I, II, III 叫做域的公理．大家都

知道，有理数的加法运算和乘法运算，实数的加法运算和乘法运算，以及复数的加法运算和乘法运算所满足的运算规则不只有 I, II, III 中这几条. 但我们说 I, II, III 这几条是最基本的，其余的一些加法和乘法运算的规则可以从它们推导出来. 因此我们把它们抽出来作为域的公理. 这样在我们验证一个定义了加法运算和乘法运算的集合是不是域时，除了验证这个集合是不是对于加法和乘法自封之外，只要验证 I, II, III 是否成立就行了，而无须检验其他运算规则是否成立. 下面我们从域的公理出发来推导域的另外一些运算规则，我们把它们归纳在下面三个定理里.

定理 1 设 F 是任意一个域. 那么

i) F 中适合条件

$$a+0=a, \quad \text{对一切 } a\in F$$

的元素 0 是唯一确定的.

ii) 对于任意 $a\in F$, F 中适合条件

$$a+(-a)=0$$

的元素 $-a$ 是唯一确定的.

iii) F 中不等于 0 而且适合条件

$$a\cdot e=a, \quad \text{对一切 } a\in F$$

的元素 e 是唯一确定的.

iv) 对于任意 $a\in F$ 而 $a\neq 0$, F 中适合条件

$$a\cdot a^{-1}=e$$

的元素 a^{-1} 是唯一确定的.

证. 设 F 中有元素 0 和 $0'$ 分别适合条件

$$a+0=a, \quad \text{对一切 } a\in F;$$

$$a+0'=a, \quad \text{对一切 } a\in F.$$

在前一式中令 $a=0'$, 有

$$0'+0=0'.$$

在后一式中令 $a=0$，有

$$0+0'=0.$$

但是根据 I.1，有

$$0'+0=0+0'.$$

因此一定有 $$0=0'.$$

这证明了 i) 成立.

对于任意 $a\in F$，设 F 中有 $-a$ 和 b 有性质

$$a+(-a)=0, \quad a+b=0.$$

那么

$$\begin{aligned} b&=b+0=b+(a+(-a))=(b+a)+(-a)\\ &=(a+b)+(-a)=0+(-a)\\ &=(-a)+0=-a. \end{aligned}$$

这证明了 ii) 成立.

完全可以平行地证明 iii) 和 iv) 也成立，我们就不重复了.

基于定理 1，我们可以给出下面这个定义.

定义 4 设 F 是任意一个域. F 中适合条件

$$a+0=a, \quad 对一切\ a\in F$$

的唯一的那个元素 0 叫做 F 的*零元素*. 对任意 $a\in F$，F 中适合条件

$$a+(-a)=0$$

的唯一的那个元素 $-a$ 叫做 a 的*负元素*. F 中适合条件

$$a\cdot e=a, \quad 对一切\ a\in F$$

的唯一的那个 $\neq 0$ 的元素 e 叫做 F 的*单位元素*. 对任意 $a\in F$ 而 $a\neq 0$，F 中适合条件

$$a\cdot a^{-1}=e$$

的唯一的那个元素 a^{-1} 叫做 a 的*逆元素*.

定理 2 设 F 是个域，那么在 F 中以下运算规则也成立:

i) 加法消去律．设 a, b, c 是 F 中任意三个元素．如果 $a+c=b+c$，那么一定有 $a=b$．

ii) 乘法消去律．设 a, b, c 是 F 中任意三个元素，而 $c\neq 0$．如果 $ac=bc$，那么一定有 $a=b$．

iii) $a\cdot 0=0$，对任意 $a\in F$．

iv) 设 $a, b\in F$．如果 $ab=0$，那么一定有 $a=0$ 或 $b=0$．

证．设 $a+c=b+c$，那么

$$a=a+0=a+(c+(-c))=(a+c)+(-c)$$
$$=(b+c)+(-c)=b+(c+(-c))=b+0=b.$$

这证明了 i)．

再设 $ac=bc$，而 $c\neq 0$，那么

$$a=a\cdot e=a\cdot(c\cdot c^{-1})=(a\cdot c)\cdot c^{-1}$$
$$=(b\cdot c)\cdot c^{-1}=b\cdot(c\cdot c^{-1})=b\cdot e=b.$$

这证明了 ii)．

对任意 $a\in F$，我们有

$$a\cdot 0+0=a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0.$$

利用 i) 可推出 $a\cdot 0=0$．这证明了 iii)．

最后，如果 $ab=0$ 而 $a\neq 0$．那么利用 ii)，可从

$$a\cdot b=0=a\cdot 0$$

推出 $b=0$，因此 iv) 也成立．

从定理 2 中的 i) 和 ii)，即加法消去律和乘法消去律，可以推出下面这个重要的事实．

系理 1 设 F 是个域，而 F_0 是 F 的一个子域．那么 F 的零元素和单位元素一定都属于 F_0，而且分别就是 F_0 的零元素和单位元素．

证．设 0 是 F 的零元素，而 0_0 是 F_0 的零元素．因为 $0_0\in F$ 而 0 是 F 的零元素，所以根据 I.3 有 $0_0+0=0_0$．又因为 0_0 是 F_0 的零元素，仍根据 I.3 有 $0_0+0_0=0_0$．因此 0_0+0

$=0_0+0_0$, 那么利用加法消去律就得出 $0=0_0$.

同样方法可平行地证明 F 的单位元素一定属于 F_0, 而且也就是 F_0 的单位元素.

从定理 2 中的 iii), 可推出下面的

系理 2 设 F 是个域, $a\in F$ 而 $a\neq 0$. 那么 a 的逆元素 a^{-1} 也一定 $\neq 0$.

证. 假定 $a^{-1}=0$, 就会有 $e=aa^{-1}=a\cdot 0=0$, 但在域的公理 II.3 中要求 $e\neq 0$. 因此一定有 $a^{-1}\neq 0$.

定理 3 设 F 是一个域. 那么在 F 中以下运算规则成立:

i) $-(-a)=a$, 对任意 $a\in F$.

ii) $-(a+b)=(-a)+(-b)$, 对任意 $a, b\in F$.

iii) $a(-b)=(-a)b=-(ab)$, 对任意 $a, b\in F$.

iv) $(-a)(-b)=ab$, 对任意 $a, b\in F$.

v) $(a^{-1})^{-1}=a$, 对任意 $a\in F$ 而 $a\neq 0$.

vi) $(ab)^{-1}=a^{-1}b^{-1}$, 对任意 $a, b\in F$ 而 $a\neq 0, b\neq 0$.

vii) $(-a)^{-1}=-a^{-1}$, 对任意 $a\in F$ 而 $a\neq 0$.

证. 我们有

$$a+(-a)=0,\quad -(-a)+(-a)=0.$$

因此

$$-(-a)+(-a)=a+(-a).$$

再利用加法消去律, 从上式就推出

$$-(-a)=a.$$

这证明了 i).

其次, 我们有

$$\begin{aligned}&(a+b)+[(-a)+(-b)]\\=&[(a+b)+(-a)]+(-b)\\=&[(b+a)+(-a)]+(-b)\\=&[b+(a+(-a))]+(-b)\\=&(b+0)+(-b)=b+(-b)=0.\end{aligned}$$

但是另一方面，显然有

$$(a+b)+[-(a+b)]=0.$$

因此有

$$(a+b)+[-(a+b)]$$
$$=(a+b)+[(-a)+(-b)],$$

再利用加法消去律就推出

$$-(a+b)=(-a)+(-b).$$

这证明了 ii).

我们有

$$0=a\cdot 0=a\cdot(b+(-b))=ab+a(-b).$$

另一方面，显然有

$$0=ab+(-(ab)).$$

因此

$$ab+a(-b)=ab+(-(ab)),$$

再利用加法消去律就推出

$$a(-b)=-(ab).$$

同理可证 $(-a)\cdot b=-(ab)$. 因此 iii) 也成立.

利用 iii) 和 i) 又可推出

$$(-a)(-b)=-(a\cdot(-b))=-(-(ab))=ab.$$

因此 iv) 也成立.

v) 和 vi) 可分别仿照 i) 和 ii) 的证明证之，我们就不重复了.

至于 vii)，对任意 $a\in F$ 而 $a\neq 0$，根据 iv) 我们有

$$(-a)(-a^{-1})=aa^{-1}=e.$$

因此有

$$(-a)^{-1}=-a^{-1}.$$

这样定理 3 就完全证明了.

在本节开始时，我们就曾指出，在有理数域中，利用相反数和倒数可以将减法运算和除法运算分别用加法运算和乘法运算表出. 在任意域 F 中，我们也可以利用负元素和逆元素来引进减法和除法. 即，如果 a, $b\in F$，那么定义

$$a-b=a+(-b).$$

更设 $b\neq 0$, 那么定义

$$a\div b=ab^{-1}.$$

从域中加法运算和乘法运算所满足的运算规则，即域的公理和上面的三条定理中的规则，还可以推出域中加、减、乘、除四则运算所满足的有理数域中四则运算的另一些规则. 例如，对域 F 中任意三个元素 a, b, c, 我们有

$$a-(b+c)=a-b-c,$$

$$a-(b-c)=a-b+c,$$

$$a(b-c)=ab-ac,$$

$$a\div(bc)=ab^{-1}c^{-1}, \quad \text{如果 } b\neq 0,\ c\neq 0,$$

$$a\div(b\div c)=ab^{-1}c, \quad \text{如果 } b\neq 0,\ c\neq 0,$$

等等.

设 a 是域 F 中任意元素，而 n 是任意正整数，我们还约定把 n 个 a 之和

$$\underbrace{a+a+\cdots+a}_{n\text{个}a}$$

简记作 na, 即定义

$$na=\underbrace{a+a+\cdots+a}_{n\text{个}}.$$

并规定 0 个 a 是 F 中的零元素 0, 即

$$0a=0.$$

注意上式左侧的 0 是整数 0, 而右侧的 0 是域 F 中的零元素. 仍设 n 是正整数，那么 $-n$ 是负整数，我们定义

$$(-n)a=-(na).$$

那么我们有以下这些运算规则:

i) 对任意 $a\in F$, 任意整数 m 和 n, 都有

$$(m+n)a=ma+na,\ (mn)a=m(na).$$

ii) 对任意 $a, b\in F$, 任意整数 n, 都有

$$n(a+b)=na+nb.$$

iii) 对任意 $a, b\in F$, 任意整数 m 和 n, 都有

$$(ma)(nb)=(ma)(ab).$$

仍设 a 是域 F 中任意元素，而 n 是任意正整数. 我们还约定把 n 个 a 之积

$$\underbrace{a\cdot a\cdot\cdots\cdot a}_{n\text{ 个 }a}$$

简记作 a^n, 即定义

$$a^n=\underbrace{a\cdot a\cdot\cdots\cdot a}_{n\text{ 个 }a}.$$

当 $a\neq 0$ 时，我们还规定

$$a^0=e,$$

$$a^{-n}=(a^{-1})^n.$$

那么我们有下面这些运算规则:

i) 对任意 $a\in F$, 任意整数 m 和 n, 都有

$$a^{m+n}=a^m\cdot a^n,$$

$$a^{mn}=(a^m)^n.$$

而当 $a=0$ 时，我们还要求 m 和 n 都 >0.

ii) 对任意 $a, b\in F$, 任意整数 m, 都有

$$(ab)^m=a^m\cdot b^m,$$

而当 $a=0$ 或 $b=0$ 时，我们还要求 $m>0$.

iii) 二项式定理. 对任意 $a, b\in F$, 任意正整数 n, 都有

$$(a+b)^n=\sum_{i=0}^{n}\binom{n}{i}a^ib^{n-i},$$

式中 $\binom{n}{i}$ 是从 n 个两两相异的对象中取出 i 个来的方法数，亦称 n 中取 i 的组合数，即

$$\binom{n}{i}=\frac{n!}{i!(n-i)!}.$$

上面这些运算规则的证明，除了二项式定理之外，都非常容易. 至于二项式定理的证明，在任何一本中学代数课本上都可以找到，那里的证明可以原封不动地搬到任意域上来. 因此我们就不重复了.

§2 多项式和有理分式

设 F 是一个预先给定的域，而 x 是一个符号(或称文字). 设 i 是个非负整数，形如

$$a_i x^i, \quad a_i \in F$$

的式子，叫做系数属于 F 的(符号) x 的单项式. 而有限个系数属于 F 的单项式 a_0x^0, a_1x^1, a_2x^2, $\cdots$, a_nx^n (其中 n 是任意非负整数而 $a_0, a_1, a_2, \cdots, a_n \in F$)的形式和

$$a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n \tag{1}$$

就叫做系数属于 F 的 x 的多项式，或简称域 F 上的 x 的多项式. 在多项式(1)中，a_ix^i 叫做它的 i 次项，a_i 叫做它的 i 次项的系数. 当 $a_i = e$ 时，记 $ex^i = x^i$. 今后我们约定 $x^0 = e$ 为 F 中的单位元素，记 a_0x^0 为 a_0，并将 x^1 记作 x，那么多项式(1)又可写作

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

我们往往用省略记号 $f(x)$, $g(x)$, $h(x)$; $f_i(x)$, $\cdots$ 等等来代表多项式.

设 $f(x)$ 和 $g(x)$ 是 F 上的 x 的两个多项式. 如果除去系数等于域 F 中的零元素 0 的项以外，它们同次项的系数都相等，我们就说 $f(x)$ 和 $g(x)$ 相等，也说 $f(x)$ 和 $g(x)$ 是同一个多项式，记作

$$f(x) = g(x).$$

特别，$\quad a_0 + a_1x + a_2x^2 + \cdots + a_ix^n, \quad a_i \in F$

和 $$a_0+a_1x+a_2x^2+\cdots+a_nx^n+0\cdot x^{n+1}$$
$$+0\cdot x^{n+2}+\cdots+0\cdot x^{n+m}$$
是相等的多项式.

下面我们往往采用求和记号 $\sum$ 来将多项式
$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$
简记作 $$f(x)=\sum_{i=0}^{n}a_ix^i.$$
如果 $a_n\neq 0$，我们就说 $f(x)$ 是 n 次多项式，记作 $\partial^0 f(x)=n$，并说 a_n 是 $f(x)$ 的首项系数. 当 $f(x)$ 的所有系数都是 0 时，我们就说 $f(x)$ 是零多项式，仍用 0 来代表它，并规定 $\partial^0 0=-\infty$.

我们把 F 上 x 的多项式的全体所组成的集合记作 $F[x]$. 下面我们来规定 $F[x]$ 中的加法运算和乘法运算. 设 $f(x)$ 和 $g(x)$ 是 $F[x]$ 中任意两个元素，并设
$$f(x)=\sum_{i=0}^{n}a_ix^i,\quad g(x)=\sum_{i=0}^{m}b_ix^i.$$
令 $M=\max(n,\ m)$，即当 $n\neq m$ 时，M 就是 n 和 m 中较大的那个数，而当 $n=m$ 时，$M=n=m$. 置
$$a_{n+1}=a_{n+2}=\cdots=a_M=0,\quad 如果\ n<M,$$
$$b_{m+1}=b_{m+2}=\cdots=b_M=0,\quad 如果\ m<M.$$
那么可以将 $f(x)$ 和 $g(x)$ 写成
$$f(x)=\sum_{i=0}^{M}a_ix^i,\quad g(x)=\sum_{i=0}^{M}b_ix^i.$$
我们按下式来规定 $f(x)$ 和 $g(x)$ 的和，并将这个和记作
$$f(x)+g(x)=\sum_{i=0}^{M}(a_i+b_i)x^i.$$
显然 $f(x)+g(x)\in F[x]$，即 $F[x]$ 对于如上所定义的加法运算是自封的. 再置
$$a_{n+1}=a_{n+2}=\cdots=a_{n+m}=0,\quad 如果\ m\geqslant 1,$$

$$b_{m+1}=b_{m+2}=\cdots=b_{m+n}=0,\quad \text{如果 } n\geqslant 1.$$

那么可以将 $f(x)$ 和 $g(x)$ 写成

$$f(x)=\sum_{i=0}^{n+m}a_ix^i,\quad g(x)=\sum_{i=0}^{n+m}b_ix^i.$$

我们按下式来规定 $f(x)$ 与 $g(x)$ 之积，并将这个积记作

$$f(x)\cdot g(x)=\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}a_jb_{i-j}\right)x^i.$$

显然 $f(x)\cdot g(x)\in F[x]$，即 $F[x]$ 对于如上所定义的乘法运算是自封的．更进一步还可以证明

$$\partial^0(f(x)+g(x))\leqslant\max(\partial^0f(x),\ \partial^0g(x)),$$
$$\partial^0(f(x)\cdot g(x))=\partial^0f(x)+\partial^0g(x).$$

不难验证如上所规定的 $F[x]$ 中的加法运算和乘法运算满足运算规则 I.1, I.2, I.3, I.4, II.1, II.2, II.3 和 III. 但在 $F[x]$ 中，II.4 却不成立．实际上，x 在 $F[x]$ 中就没有逆元素．如果 $f(x)\in F[x]$ 是 x 的逆元素，即 $x\cdot f(x)=e$，那么 $\partial^0(xf(x))=\partial^0e$．但 $\partial^0(xf(x))=\partial^0x+\partial^0f(x)\geqslant\partial^0x=1$，而 $\partial^0e=0$．这是不可能的．既然在 $F[x]$ 中 II.4 不成立，因此 $F[x]$ 不是域．

因为 $F[x]$ 中有 $\neq 0$ 的元素在 $F[x]$ 中没有逆元素，所以不能象 §1 中对于域所做的那样，利用逆元素通过乘法运算来引进除法．但是和 $\mathbf{Z}$ 中一样，$F[x]$ 中也有带余除法．

定理1 （带余除法）设 $a(x)$ 和 $b(x)$ 是 $F[x]$ 中的两个多项式，而 $b(x)\neq 0$．那么 $F[x]$ 中有唯一的一对多项式 $q(x)$ 和 $r(x)$ 具有下面的性质：

$$a(x)=q(x)b(x)+r(x),\quad \partial^0r(x)<\partial^0b(x).\tag{2}$$

证．先对 $a(x)$ 的次数用归纳法来证明 $F[x]$ 中有一对具有性质(2)的多项式 $q(x)$ 和 $r(x)$．

当 $\partial^0a(x)<\partial^0b(x)$ 时，取 $q(x)=0$，$r(x)=a(x)$，(2)就

成立.

当 $\partial^0 a(x) > \partial^0 b(x)$ 时，设

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$
$$b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m,$$

$a_n \neq 0$, $b_m \neq 0$. 那么 $n > m$. 令

$$a_1(x) = a(x) - a_n b_m^{-1} x^{n-m} b(x)$$

那么 $\partial^0 a_1(x) \leqslant n-1$. 根据归纳法假设，$F[x]$ 中有一对多项式 $q_1(x)$ 和 $r_1(x)$ 使

$$a_1(x) = q_1(x) b(x) + r_1(x),$$
$$\partial^0 r_1(x) < \partial^0 b(x).$$

于是 $$a(x) = [a_n b_m^{-1} x^{n-m} + q_1(x)] b(x) + r_1(x).$$

令 $$q(x) = a_n b_m^{-1} x^{n-m} + q_1(x), \quad r(x) = r_1(x),$$

就有(2)式.

再证明具有性质(2)的多项式对 $q(x)$ 和 $r(x)$ 是唯一的. 设有另一对多项式 $q_1(x)$ 和 $r_1(x)$ 使

$$a(x) = q_1(x) b(x) + r_1(x),$$
$$\partial^0 r_1(x) < \partial^0 b(x).$$

那么 $$(q(x) - q_1(x)) b(x) = -r(x) + r_1(x).$$

于是 $$\partial^0 [(q(x) - q_1(x)) \cdot b(x)] = \partial^0 (-r(x) + r_1(x)).$$

但

$$\partial^0 (-r(x) + r_1(x)) \leqslant \max(\partial^0 r(x), \partial^0 r_1(x)) < \partial^0 b(x),$$

因此 $$\partial^0 [q(x) - q_1(x)) \cdot b(x)]$$
$$= \partial^0 (q(x) - q_1(x)) + \partial^0 b(x) < \partial^0 b(x),$$

所以一定有 $q(x) - q_1(x) = 0$, 即 $q(x) = q_1(x)$. 因而也有 $r(x) = r_1(x)$. 这证明了定理 1.

定理 1 中所得到的 $q(x)$ 叫做用 $b(x)$ 做除式去除被除式 $a(x)$ 所得的商，而 $r(x)$ 叫做用 $b(x)$ 去除 $a(x)$ 所得的余式. 我们记

$$r(x)=(a(x))_{b(x)},$$

而(2)就叫带余除法算式.

系理 设 $a_1(x)$, $a_2(x)$ 和 $b(x)$ 都是 $F[x]$ 中的多项式, 而 $b(x)\neq 0$. 那么

$$(a_1(x)\pm a_2(x))_{b(x)}=(a_1(x))_{b(x)}\pm(a_2(x))_{b(x)},$$

$$(a_1(x)\cdot a_2(x))_{b(x)}=((a_1(x))_{b(x)}\cdot(a_2(x))_{b(x)})_{b(x)}.$$

证. 根据定理 1, 设

$$a_1(x)=q_1(x)b(x)+(a_1(x))_{b(x)},$$

$$\partial^0(a_1(x))_{b(x)}<\partial^0 b(x),$$

$$a_2(x)=q_2(x)b(x)+(a_2(x))_{b(x)},$$

$$\partial^0(a_2(x))_{b(x)}<\partial^0 b(x),$$

那么
$$a_1(x)\pm a_2(x)=(q_1(x)\pm q_2(x))b(x)$$
$$+(a_1(x))_{b(x)}\pm(a_2(x))_{b(x)}.$$

因
$$\partial^0((a_1(x))_{b(x)}\pm(a_2(x))_{b(x)})$$
$$\leqslant\max(\partial^0(a_1(x))_{b(x)},\ \partial^0(a_2(x))_{b(x)})<\partial^0 b(x),$$

那么根据余式的唯一性就有

$$(a_1(x)\pm a_2(x))_{b(x)}=(a_1(x))_{b(x)}\pm(a_2(x))_{b(x)}.$$

其次, 我们有

$$a_1(x)\cdot a_2(x)=(q_1(x)q_2(x)b(x)$$
$$+q_1(x)(a_2(x))_{b(x)}+q_2(x)(a_1(x))_{b(x)})b(x)$$
$$+(a_1(x))_{b(x)}(a_2(x))_{b(x)},$$

根据定理 1, 可设

$$(a_1(x))_{b(x)}(a_2(x))_{b(x)}=q_3(x)b(x)$$
$$+((a_1(x))_{b(x)}(a_2(x))_{b(x)})_{b(x)},$$

那么
$$a_1(x)\cdot a_2(x)=(q_1(x)q_2(x)b(x)$$
$$+q_1(x)(a_2(x))_{b(x)}+q_2(x)(a_1(x))_{b(x)}$$
$$+q_3(x))b(x)+((a_1(x))_{b(x)}(a_2(x))_{b(x)})_{b(x)}.$$

但
$$\partial^0((a_1(x))_{b(x)}(a_2(x))_{b(x)})_{b(x)}<\partial^0 b(x),$$

仍根据余式的唯一性就有

$$(a_1(x)\cdot a_2(x))_{b(x)}=((a_1(x))_{b(x)}(a_2(x))_{b(x)})_{b(x)}.$$

这个系理也可以推广到 n 个多项式 $a_i(x)$ $(i=1, 2, \cdots, r)$ 的和与积的情形，即

$$(a_1(x)+a_2(x)+\cdots+a_n(x))_{b(x)}$$
$$=(a_1(x))_{b(x)}+(a_2(x))_{b(x)}+\cdots+(a_n(x))_{b(x)},$$
$$(a_1(x)\cdot a_2(x)\cdots\cdots a_n(x))_{b(x)}$$
$$=((a_1(x))_{b(x)}\cdot(a_2(x))_{b(x)}\cdots,\ (a_n(x))_{b(x)})_{b(x)}.$$

这两个式子的证明请读者自己补出. 定理 1 的系理和上面这两个式子以后经常用到，希望读者能把它们记住.

还应该指出，定理 1 中的归纳证明实际上给出了具体求 $q(x)$ 和 $r(x)$ 的方法. 我们举一个例子来阐明这一点. 设 $F=\mathbf{Z}_2$，在 $\mathbf{Z}_2[x]$ 中取

$$a(x)=x^5+x^4+x^2+1,$$
$$b(x)=x^3+x+1,$$

我们可以按照下面的算式(通常叫做竖式)来进行带余除法：

$$\begin{array}{r|l|l}
x^3+x+1 & x^5+x^4\qquad\quad +x^2\quad +1 & x^2+x+1 \\
 & x^5\qquad\quad +x^3+x^2 & \\ \hline
 & \qquad x^4\quad +x^3\qquad\quad +1 & \\
 & \qquad x^4\qquad\quad +x^2+x & \\ \hline
 & \qquad\qquad\quad x^3+x^2+x+1 & \\
 & \qquad\qquad\quad x^3\qquad +x+1 & \\ \hline
 & \qquad\qquad\qquad x^2 &
\end{array}$$

于是求得商 $\qquad q(x)=x^2+x+1$

和余式 $\qquad r(x)=x^2$

所得结果可以写成横式

$$x^5+x^4+x^2+1=(x^2+x+1)(x^3+x+1)+x^2.$$

为了书写和计算的方便，我们约定将 $F[x]$ 中的 n 次多项式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

简记作 $$a_na_{n-1}\cdots a_1a_0.$$

例如，可以把 $\mathbf{Z}_2[x]$ 中的多项式

$$x^5+x^4+x^2+1$$

和 $$x^3+x+1,$$

分别简记作 $$1\ 1\ 0\ 1\ 0\ 1$$

和 $$1\ 0\ 1\ 1,$$

同时，上面用 x^3+x+1 去除 $x^5+x^4+x^2+1$ 的带余除法的竖式也可以用下面的简式来代替：

```
1 0 1 1 | 1 1 0 1 0 1 | 1 1 1
        | 1 0 1 1     |
        | ----------- |
        |   1 1 0 0 1 |
        |   1 0 1 1   |
        |   --------- |
        |     1 1 1 1 |
        |     1 0 1 1 |
        |     ------- |
        |         1   |
```

既然 $F[x]$ 和 $\mathbf{Z}$ 一样也有带余除法，所以也可以平行地讨论 $F[x]$ 中的整除性、因式、倍式、最高公因式、最低公倍式和不可约多项式等概念.

首先，当(2)中的 $r(x)=0$ 时，我们就说 $b(x)$ 是 $a(x)$ 的因式，或 $a(x)$ 是 $b(x)$ 的倍式，也说 $a(x)$ 被 $b(x)$ 所整除，或 $b(x)$ 除得尽 $a(x)$，并用符号

$$b(x)\,|\,a(x)$$

来表示．我们还用符号

$$b(x)\nmid a(x)$$

来表示 $b(x)$ 除不尽 $a(x)$，即用 $b(x)$ 去除 $a(x)$ 所得的余式 $\neq 0$．显然如果 $b(x)$ 是 $a(x)$ 的因式而 $a(x)\neq 0$，那么一定有

$$\partial^0 b(x)\leqslant\partial^0 a(x).$$

设 $a(x)$，$b(x)$，$c(x)$ 都是 $F[x]$ 中的多项式，而 $c(x)\neq 0$．如果 $c(x)$ 既是 $a(x)$ 的因式，又是 $b(x)$ 的因式，我们就说 $c(x)$ 是 $a(x)$ 和 $b(x)$ 的**公因式**．当 $a(x)$ 和 $b(x)$ 不全等于 0 时，$a(x)$ 和 $b(x)$ 的公因式中就有一个次数最高的而首项系数等于 e 的；我们把它叫做 $a(x)$ 和 $b(x)$ 的**最高公因式**，并用符号

$$(a(x),\ b(x))$$

来表示．当 $a(x)$ 和 $b(x)$ 都等于 0 时，那么任何一个多项式都是它们的公因式，这时 a 和 b 没有最高公因式，因此符号 $(0,\ 0)$ 没有意义．

设 $a(x)$ 和 $b(x)$ 都是 $F[x]$ 中不等于 0 的多项式．我们也可以用**辗转相除法**来求 $(a(x),\ b(x))$．根据带余除法，用 $b(x)$ 去除 $a(x)$ 得到商 $q_1(x)$ 和余式 $r_1(x)$．如果 $r_1(x)\neq 0$，再用 $r_1(x)$ 去除 $b(x)$ 得到商 $q_2(x)$ 和余式 $r_2(x)$．如果 $r_2(x)\neq 0$，又用 $r_2(x)$ 去除 $r_1(x)$ 得到商 $q_3(x)$ 和余式 $r_3(x)$．这样辗转相除下去，显然所得到的余式的次数不断降低，即

$$\partial^0 b(x)>\partial^0 r_1(x)>\partial^0 r_2(x)>\cdots,$$

因此在有限次之后，必然有余式为 0．于是我们有下面这一串式子

$$\begin{aligned}
a(x)&=q_1(x)b(x)+r_1(x),\ 0\leqslant\partial^0 r_1(x)<\partial^0 b(x),\\
b(x)&=q_2(x)r_1(x)+r_2(x),\ 0\leqslant\partial^0 r_2(x)<\partial^0 r_1(x),\\
r_1(x)&=q_3(x)r_2(x)+r_3(x),\ 0\leqslant\partial^0 r_3(x)<\partial^0 r_2(x),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,
\end{aligned}\tag{3}$$

$$r_{n-3}(x)=q_{n-1}(x)r_{n-2}(x)+r_{n-1}(x),$$
$$0\leqslant\partial^0 r_{n-1}(x)<\partial^0 r_{n-2}(x),$$
$$r_{n-2}(x)=q_n(x)r_{n-1}(x)+r_n(x),$$
$$0\leqslant\partial^0 r_n(x)<\partial^0 r_{n-1}(x),$$
$$r_{n-1}(x)=q_{n+1}(x)r_n(x).$$

设 $r_n(x)$ 的首项系数是 c, 那么

$$(a(x),\ b(x))=c^{-1}r_n(x).$$

上面这个式子的证明完全和附录二中关于整数的情形完全一样,我们就不重复了. 另外,和附录二中关于整数的情形完全一样,利用上面这一串式子,还可以将 $a(x)$ 和 $b(x)$ 的最高公因式 $(a(x),\ b(x))$ 表成 $a(x)$ 和 $b(x)$ 的多项式系数的线性组合,即

$$(a(x),\ b(x))=c(x)a(x)+d(x)b(x), \tag{4}$$

其中 $c(x)$ 和 $d(x)$ 都是 $F[x]$ 中的多项式. 那么从上面这个式子立刻推出 $a(x)$ 和 $b(x)$ 的任一公因式都是 $(a(x),\ b(x))$ 的因式.

定理 2 设 F 是域,而 $a(x)$ 和 $b(x)$ 是 $F[x]$ 中不等于 0 的多项式, 那么 $a(x)$ 和 $b(x)$ 的最高公因式 $(a(x),\ b(x))$ 可以表成 $a(x)$ 和 $b(x)$ 的以 $F[x]$ 中多项式为系数的线性组合, 即

$$(a(x),\ b(x))=c(x)a(x)+d(x)b(x) \tag{4}$$

其中 $c(x)$ 和 $d(x)$ 都是 $F[x]$ 中的多项式, 而且 $a(x)$ 和 $b(x)$ 的任一公因式都是$(a(x),\ b(x))$的因式. 更进一步, 如果再假定 $\partial^0 a(x)>0$ 和 $\partial^0 b(x)>0$ 同时 $a(x)\neq c\cdot b(x)$ 对任一 $c\in F$, 那么还可以要求(4)中的 $c(x)$ 和 $d(x)$ 适合条件

$$\partial^0 c(x)<\partial^0 b(x)-\partial^0(a(x),\ b(x)),$$
$$\partial^0 d(x)<\partial^0 a(x)-\partial^0(a(x),\ b(x)); \tag{5}$$

而且适合上述条件的 $c(x)$ 和 $d(x)$ 是唯一的.

证．唯一还需要证明的就是本定理的最后一个断言．

已知(4)式成立，而其中的 $c(x)$ 和 $d(x)$ 不一定适合条件(5)．令

$$a(x)=a_1(x)(a(x),\ b(x)),$$

$$b(x)=b_1(x)(a(x),\ b(x)),$$

那么
$$\partial^0 a_1(x)=\partial^0 a(x)-\partial^0(a(x),\ b(x)),$$

$$\partial^0 b_1(x)=\partial^0 b(x)-\partial^0(a(x),\ b(x)).$$

根据带余除法，有

$$c(x)=q_1(x)b_1(x)+c_1(x),\ \partial^0 c_1(x)<\partial^0 b_1(x),$$

$$d(x)=q_2(x)a_1(x)+d_1(x),\ \partial^0 d_1(x)<\partial^0 a_1(x).$$

于是
$$(a(x),\ b(x))=(q_1(x)+q_2(x))a_1(x)b_1(x)\cdot(a(x),\ b(x))+c_1(x)a(x)+d_1(x)b(x). \tag{6}$$

令
$$n=\partial^0 a(x)+\partial^0 b(x)-\partial^0(a(x),\ b(x)),$$

那么
$$n=\partial^0 a_1(x)+\partial^0 b_1(x)+\partial^0(a(x),\ b(x)).$$

显然有
$$\partial^0(c_1(x)a(x)+d_1(x)b(x))<n.$$

又因 $a(x)\neq cb(x)$，对任一 $c\in F$，所以

$$\partial^0 a_1(x)+\partial^0 b_1(x)>0,$$

因此
$$\partial^0(a(x),\ b(x))<n.$$

但是
$$\partial^0(a_1(x)b_1(x)(a(x),\ b(x)))=n.$$

于是由(6)式推出

$$q_1(x)+q_2(x)=0.$$

因此
$$(a(x),\ b(x))=c_1(x)a(x)+d_1(x)b(x),$$

而
$$\partial^0 c_1(x)<\partial^0 b_1(x)=\partial^0 b(x)-\partial^0(a(x),\ b(x)),$$

$$\partial^0 d_1(x)<\partial^0 a_1(x)=\partial^0 a(x)-\partial^0(a(x),\ b(x)).$$

至于适合条件(5)的 $c(x)$ 和 $d(x)$ 的唯一性，我们放在后面去证明.

当 $a(x)$ 和 $b(x)$ 的最高公因式是 e 时，即当 $(a(x), b(x))=e$ 时，我们就说 $a(x)$ 和 $b(x)$ **互素**. 我们有

系理 设 F 是域，而 $a(x)$ 和 $b(x)$ 是 $F[x]$ 中两个互素的多项式，那么一定有 $F[x]$ 中的多项式 $c(x)$ 和 $d(x)$ 使

$$e=c(x)a(x)+d(x)b(x).$$

更进一步，如果再假定 $a(x)$ 和 $b(x)$ 都是次数 $\geqslant 1$ 的多项式，那么还可以要求

$$\partial^0 c(x)<\partial^0 b(x),\ \partial^0 d(x)<\partial^0 a(x).$$

我们举一个实例来阐明怎样用辗转相除法来求两个多项式的最高公因式，以及怎样将最高公因式表成它们的线性组合. 例如，求 $\mathbf{Z}_2[x]$ 中多项式

$$x^5+x^4+x^3+x^2+x+1 \quad 和 \quad x^4+x^2+x+1$$

的最高公因式，可采用下面的算式(通常称为竖式)来进行辗转相除:

$$
\begin{array}{r|r|r|l}
x^2+x & x^4 \qquad +x^2+x+1 & x^5+x^4+x^3+x^2+x+1 & x+1 \\
 & x^4+x^3 \qquad\qquad & x^5 \qquad +x^3+x^2+x \quad & \\
\cline{2-3}
 & x^3+x^2+x+1 & x^4 \qquad\qquad +1 & \\
 & x^3+x^2 \qquad\quad & x^4 \qquad +x^2+x+1 & \\
\cline{2-3}
 & x+1 & x^2+x \qquad & x \\
 & & x^2+x \qquad & \\
\cline{3-3}
 & & 0 \qquad\quad &
\end{array}
$$

这样 $\quad x+1=(x^5+x^4+x^3+x^2+x+1,\ x^4+x^2+x+1).$

也可以将上面辗转相除法的竖式用下面的简式来代替

1 1 0	1 0 1 1 1	1 1 1 1 1 1	1 1
	1 1	1 0 1 1 1	
	1 1 1 1	1 0 0 0 1	
	1 1	1 0 1 1 1	
	1 1	1 1	1
		1 1	
		0	

为了将$x+1$表成$x^5+x^4+x^3+x^2+x+1$和x^4+x^2+x+1的线性组合，需要先把上面辗转相除法的竖式先改写成横式

$$x^5+x^4+x^3+x^2+x+1$$
$$=(x+1)(x^4+x^2+x+1)+(x^2+x),$$
$$x^4+x^2+x+1=(x^2+x)(x^2+x)+(x+1),$$
$$x^2+x=x(x+1).$$

那么

$$\begin{aligned} x+1 &= (x^4+x^2+x+1)+(x^2+x)(x^2+x) \\ &= (x^4+x^2+x+1)+(x^2+x)[(x^5+x^4+x^3+x^2+x+1) \\ &\quad +(x+1)\cdot(x^4+x^2+x+1)] \\ &= (x^2+x)(x^5+x^4+x^3+x^2+x+1) \\ &\quad +(x^3+x+1)(x^4+x^2+x+1). \end{aligned}$$

再设$a(x)$, $b(x)$, $c(x)$都是$F[x]$中的多项式而$a(x)\neq 0$, $b(x)\neq 0$. 如果$c(x)$既是$a(x)$的倍式，又是$b(x)$的倍式，我们就说$c(x)$是$a(x)$和$b(x)$的公倍式. 显然$a(x)\ b(x)$是$a(x)$和$b(x)$的一个公倍式. 因此$a(x)$和$b(x)$的公倍式中一定有一个次数最低的而首项系数等于e的，我们把它叫做$a(x)$和$b(x)$的最低公倍式，并用符号

$$[a(x),\ b(x)]$$

来表示它.

和整数的情形一样，对于 $F[x]$ 中有限多个不全 $=0$ 的多项式 $a_1(x), a_2(x), \cdots, a_n(x)$ 也可以定义它们的最高公因式，并把它记作 $(a_1(x), a_2(x), \cdots, a_n(x))$. 当 $a_i(x)(1\leqslant i\leqslant n)$ 都不等于 0 时，也可以定义它们的最低公倍式，并把它记作 $[a_1(x), a_2(x), \cdots, a_n(x)]$. 细节我们就不重复了.

设 $p(x)$ 是 $F[x]$ 中的一个次数 $\geqslant 1$ 的多项式，如果 $p(x)$ 在 $F[x]$ 中的因式只有 F 中的 $\neq 0$ 的元素 c 和 $cp(x)$，我们说 $p(x)$ 是 $F[x]$ 中的一个**不可约多项式**. 否则 $p(x)$ 就叫做 $F[x]$ 中的**可约多项式**. 显然 $F[x]$ 中的一个次数 $\geqslant 1$ 的多项式 $p(x)$ 是不可约的，当且仅当 $p(x)$ 不能表成(或说分解成) $F[x]$ 中两个次数 $<\partial^0 p(x)$ 的多项式的乘积. 多项式的可约、不可约的概念是与域的概念密切相关的. 举例来说，x^2-2 是 $\mathbf{Q}[x]$ 中的不可约多项式；但在 $\mathbf{R}[x]$ 中，x^2-2 却是可约的，因为在 $\mathbf{R}[x]$ 中，

$$x^2-2=(x+\sqrt{2})(x-\sqrt{2}),$$

那么 $x+\sqrt{2}$ 和 $x-\sqrt{2}$ 都是 x^2-2 的因式.

平行于算术基本定理，我们有

定理 3 (唯一因式分解定理)域 F 上任一次数 $\geqslant 1$ 的多项式 $f(x)$ 都可以表成 $F[x]$ 中一些不可约多项式的乘积. 更进一步，如果

$$f(x)=p_1(x)p_2(x)\cdots p_r(x)=q_1(x)q_2(x)\cdots q_s(x)$$

是将 $f(x)$ 分解成不可约多项式之积的两种方法，那么一定有 $r=s$ 并且适当重排因式的次序之后有

$$p_i(x)=c_i q_i(x),$$

其中 $c_i(i=1, 2, \cdots, r)$ 是 F 中一些 $\neq 0$ 的元素.

这个定理的证明与附录二中算术基本定理的证明完全平行. 在证明定理的第一部分时，可以对 $f(x)$ 的次数作数学归

纳法．在证明定理的第二部分时，要对 r 作归纳法；当然在证明中要用到下面这个与附录二中引理1相平行的一条引理．

引理 1 设 $p(x)$ 是 $F[x]$ 中的一个不可约多项式而 $p(x)\mid a(x)b(x)$，其中 $a(x)$ 和 $b(x)$ 都是 $F[x]$ 中的多项式．那么 $p(x)\mid a(x)$ 或 $p(x)\mid b(x)$．

这个引理的证明也和附录二中引理1的证明完全一样，我们就不重复了．我们将证明它的一个推广．

引理 2 设 $f(x)$，$a(x)$，$b(x)$ 都是 $F[x]$ 中的多项式，而 $f(x)\neq 0$．如果 $f(x)\mid a(x)b(x)$，而 $(f(x), a(x))=e$，那么 $f(x)\mid b(x)$．

证．因 $(f(x), a(x))=e$，根据定理2的系理可知有 $F[x]$ 中的多项式 $c(x)$ 和 $d(x)$ 使

$$e=c(x)f(x)+d(x)a(x).$$

将上式双方乘以 $b(x)$，得

$$b(x)=b(x)c(x)f(x)+d(x)a(x)b(x).$$

显然 $f(x)$ 是上式右方的因式，因此 $f(x)$ 也是上式左方的因式，即 $f(x)\mid b(x)$．

现在我们利用引理2去证明定理2中所遗留未证的那个断言，即假定 $\partial^0 a(x)>0$，$\partial^0 b(x)>0$ 而 $a(x)\neq cb(x)$ 对任一 $c\in F$，那么(4)式里的 $c(x)$ 和 $d(x)$，如果还适合条件(5)，就是唯一的．实际上，设还有

$$(a(x), b(x))=c_1(x)a(x)+d_1(x)b(x) \tag{7}$$

而

$$\partial^0 c_1(x)<\partial^0 b(x)-\partial^0(a(x), b(x)),$$
$$\partial^0 d_1(x)<\partial^0 a(x)-\partial^0(a(x), b(x)). \tag{8}$$

那么从(4)式减去(7)式得

$$(c(x)-c_1(x))a(x)+(d(x)-d_1(x))b(x)=0.$$

将 $a(x)$ 和 $b(x)$ 的最高公因式 $(a(x), b(x))$ 从上式中约去，得

$$(c(x)-c_1(x))a_1(x)+(d(x)-d_1(x))b_1(x)=0.$$

因 $(a_1(x),\ b_1(x))=e$，所以根据引理 2 有

$$a_1(x)\,|\,d(x)-d_1(x).$$

但是由 (5)，(8) 两式得

$$\partial^0(d(x)-d_1(x))<\partial^0 a(x)-\partial^0(a(x),\ b(x))=\partial^0 a_1(x).$$

因此 $d(x)-d_1(x)=0$，于是 $d(x)=d_1(x)$．同理可证 $c(x)=c_1(x)$．

设 $f(x)$ 和 $g(x)$ 都是 $F[x]$ 中的多项式，$f(x)\neq 0$ 而 $\partial^0 g(x)\geq 1$．如果 $g(x)^2|f(x)$，我们说 $g(x)$ 是 $f(x)$ 的一个**重因式**，我们来讨论 $F[x]$ 中一个 $\neq 0$ 的多项式 $f(x)$ 有重因式的条件．为此我们引进多项式的形式微商的概念．

设 $\quad f(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}+a_nx^n$

是 $F[x]$ 中的一个多项式．我们规定 $f(x)$ 的**形式微商** $f'(x)$ 是

$$f'(x)=a_1+2a_2x+\cdots+(n-1)a_{n-1}x^{n-2}+na_nx^{n-1}.$$

这个规定自然是受到微积分中微商的定义的启发而规定的．但在本书中，我们只把它作为一个形式定义．可以直接验证，多项式的形式微商满足以下这些基本规律：

$$(f(x)+g(x))'=f'(x)+g'(x),$$

$$(cf(x))'=cf'(x),$$

$$(f(x)\cdot g(x))'=f'(x)g(x)+f(x)g'(x),$$

$$(f(x)^m)'=mf(x)^{m-1}f'(x),$$

其中 $f(x),\ g(x)\in F[x]$，$c\in F$ 而 m 是任意正整数．

定理 4 设 $f(x)$ 是 $F[x]$ 中的一个 $\neq 0$ 的多项式，如果 $f(x)$ 与 $f'(x)$ 互素，那么 $f(x)$ 就没有重因式．

证．用反证法．设 $f(x)$ 有重因式，譬如 $g(x)$ 是它的一个重因式，$\partial^0 g(x)\geq 1$．那么可以写

$$f(x)=g(x)^2f_1(x),$$

于是 $\qquad f'(x)=2g(x)g'(x)f_1(x)+g(x)^2f_1'(x).$

因此 $g(x)$ 是 $f(x)$ 和 $f'(x)$ 的公因式，所以 $f(x)$ 和 $f'(x)$ 不互素.

设
$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$
是 $F[x]$ 中的一个多项式，而 $\alpha\in F$. 在 $f(x)$ 中用 α 代 x 得到的 F 中的元素
$$a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n$$
称为 $f(x)$ 当 $x=\alpha$ 时的值，记作 $f(\alpha)$. 利用带余除法，可以得到下面这个定理.

定理 5 （余元定理）设 $f(x)$ 是 $F[x]$ 中的多项式，而 $\alpha\in F$. 那么用一次多项式 $x-\alpha$ 去除 $f(x)$ 所得的余式是 F 中的元素 $f(\alpha)$.

证. 用 $x-\alpha$ 去除 $f(x)$，设所得的商为 $q(x)$ 而余式为 F 中的元素 c，即
$$f(x)=q(x)(x-\alpha)+c.$$
在上式中用 α 代 x 得
$$f(\alpha)=c.$$
这证明了定理 5.

如果 $F[x]$ 中的多项式 $f(x)$ 在 $x=\alpha$ 时的值 $f(\alpha)=0$，那么 α 就叫做 $f(x)$ 的一个根.

从余元定理立刻推出

系理 1 设 $f(x)$ 是 $F[x]$ 中的多项式，而 $\alpha\in F$. 那么 α 是 $f(x)$ 的根，当且仅当 $(x-\alpha)\mid f(x)$.

从系理 1 又可推出

系理 2 设 $f(x)$ 是 $F[x]$ 中的 n 次多项式. 那么 $f(x)$ 在 F 中顶多有 n 个两两相异的根.

证. 根据系理 1，$f(x)$ 在 F 中相异的根的个数等于 $f(x)$ 在 $F[x]$ 中相异的首项系数是 e 的一次因式的个数. 根据唯一因式分解定理，后者显然 $\leqslant n$.

在§1中，我们曾经选定一个素数p，构造了一个含p个元素的域，现在平行地我们选定$F[x]$中的一个不可约多项式$p(x)$，来构造一个域$F[x]_{p(x)}$. 设$p(x)$是$F[x]$中的一个n次不可约多项式. 令$F[x]_{p(x)}$表$F[x]$中所有次数$<n$的多项式的集合，即

$$F[x]_{p(x)}=\{a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}\mid a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1}\in F\}. \quad (9)$$

设$a(x)$, $b(x)\in F[x]_{p(x)}$. 我们仿照§1例4来规定$a(x)$与$b(x)$的和（将它记作$a(x)\oplus b(x)$）与积（将它记作$a(x)\odot b(x)$）：

$$a(x)\oplus b(x)=(a(x)+b(x))_{p(x)}=a(x)+b(x),$$

$$a(x)\odot b(x)=(a(x)\cdot b(x))_{p(x)}.$$

我们把$F[x]_{p(x)}$中的加法和乘法分别叫做模$p(x)$的加法和模$p(x)$的乘法. 完全和§1例4一样，可以验证$F[x]_{p(x)}$对于如上规定的加法运算和乘法运算是域. 当然在证明中要用到下面这个与§1中引理1相平行的引理和本节定理1的系理.

引理3 设$f(x)$是$F[x]$中的一个$\neq 0$的多项式，而$a(x)$和$b(x)$是$F[x]$中任意两个多项式. 那么$(a(x))_{f(x)}=(b(x))_{f(x)}$，当且仅当$f(x)\mid a(x)-b(x)$.

所有的验证细节我们都不重复了. 我们只指出，F中的零元素0就是$F[x]_{p(x)}$中的零元素，而F中的单位元素就是$F[x]_{p(x)}$中的单位元素.

还要注意，F中的元素都是$F[x]_{p(x)}$中的元素，即$F[x]_{p(x)}$中的零元素和零次多项式. 更进一步，F中任意两个元素a和b，将它们看作$F[x]_{p(x)}$中的元素进行加法运算和乘法运算得到的和$a\oplus b$与积$a\odot b$，与将它们看作F中的元素进行加法运算和乘法运算得到的和$a+b$与积$a\cdot b$是一样的，即

$$a\oplus b=(a+b)_{p(x)}=a+b,$$

$$a\odot b=(ab)_{p(x)}=a\cdot b.$$

因此 F 是 $F[x]_{p(x)}$ 的子域.

特别,如果 $p(x)$ 是 $F[x]$ 中的一个一次多项式(一次多项式一定是不可约的!),那么显然有 $F[x]_{p(x)}=F$.

更进一步,如果写

$$p(x)=p_0+p_1x+p_2x^2+\cdots+p_nx^n,\ p_i\in F,$$

那么在 $F[x]_{p(x)}$ 中有

$$p_0\oplus p_1\odot x\oplus p_2\odot x\odot x\oplus\cdots\oplus p_n\odot\underbrace{x\odot x\odot\cdots\odot x}_{n\text{个}}$$

$$=(p_0+p_1x+p_2x^2+\cdots+p_nx^n)_{p(x)}=(p(x))_{p(x)}=0.$$

这就是说 $F[x]_{p(x)}$ 中的元素 x 是 F 上的一个文字 X 的不可约多项式

$$p(X)=p_0+p_1X+p_2X^2+\cdots+p_nX^n$$

的根. 因此我们也说 $F[x]_{p(x)}$ 是添加 $F[X]$ 中一个不可约多项式 $p(X)$ 的根 x 到 F 上而得到的域.

如果 F 是 q 个元素的有限域,那么(9)中的 $a_0, a_1, a_2, \cdots, a_{n-1}$ 都可以是 F 中 q 个元素中的任一个. 因此这时 $F[x]_{p(x)}$ 是 q^n 个元素的有限域. 特别,我们取 $F=\mathbf{Z}_p$, p 是一个给定的素数, 而 $p(x)$ 是 $\mathbf{Z}_p[x]$ 中的一个 n 次不可约多项式, 那么这时 $\mathbf{Z}_p[x]_{p(x)}$ 就是一个恰含 p^n 个元素的有限域, 而包有 $\mathbf{Z}_p$ 作为它的子域. 因此在 $\mathbf{Z}_p[x]_{p(x)}$ 中也有

$$\underbrace{1\oplus 1\oplus\cdots\oplus 1}_{p\text{个}1}=0.$$

今后我们将证明:对于任意的素数 p 和正整数 n, 都存在着一个恰含 p^n 个元素的有限域, 而恰含 p^n 个元素的有限域"基本上"(以后解释)只有一个. 因此我们往往用 $\mathbf{F}_{p^n}$ 或 $GF(p^n)$ 来代表这个恰含 p^n 个元素的有限域,这并不会引起混淆.

总结以上的讨论,我们有

定理 6 设 F 是任意一个域,$p(x)$是 $F[x]$ 中的一个 n 次

不可约多项式. 令

$$F[x]_{p(x)}=\{a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}\mid a_i\in F\},$$

并对于任意 $a(x)$, $b(x)\in F[x]_{p(x)}$, 规定

$$a(x)\oplus b(x)=a(x)+b(x),$$

$$a(x)\odot b(x)=(a(x)\cdot b(x))_{p(x)}.$$

那么 $F[x]_{p(x)}$ 对于如上规定的加法运算和乘法运算是一个域,它包有 F 作子域, 而且 $F[x]_{p(x)}$ 中的元素 x 是 F 上一个文字 X 的不可约多项式 $p(X)$ 的一个根. 更进一步, 如果 F 是 q 个元素的有限域,那么 $F[x]_{p(x)}$ 就是 q^n 个元素的有限域.

现在设 $p=2$, 考察 $\mathbf{Z}_2[x]$ 中的多项式

$$p(x)=x^2+x+1.$$

因为 $p(0)=1\neq0$, $p(1)=1\neq0$, 所以 $p(x)$ 在 $\mathbf{Z}_2$ 中没有根. 又因 $p(x)$ 是 2 次的,所以 $p(x)$ 是 $\mathbf{Z}_2[x]$ 中的不可约多项式. 根据上面的一般性讨论可知 $\mathbf{Z}_2[x]_{x^2+x+1}$ 是恰含 $2^2=4$ 个元素的有限域. 实际上,

$$\mathbf{Z}_2[x]_{x^2+x+1}=\{0,\ 1,\ x,\ x+1\}.$$

根据 $\mathbf{Z}_2[x]_{x^2+x+1}$ 中加法和乘法的定义, 容易写出 $\mathbf{Z}_2[x]_{x^2+x+1}$ 的加法表和乘法表:

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\odot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

值得注意的是, $\mathbf{F}_{2^2}=\mathbf{Z}_2[x]_{x^2+x+1}$ 中任一 $\neq0$ 的元素 $\alpha(\alpha=1, x$ 或 $x+1)$ 均适合条件

$$\alpha^{2^2-1}=\alpha^3=1,$$

而 $\mathbf{F}_{2^2}$ 中有两个 $\neq0$ 的元素 x 和 $x+1$ 有性质

$$x\neq 1,\qquad x^2\neq 1,$$
$$x+1\neq 1,\quad (x+1)^2\neq 1.$$

因此 $\mathbf{F}_{2^2}$ 中 $\neq 0$ 的元素可表成它们之中任一个的幂次. 譬如,

$$x,\ x^2=x+1,\ x^3=1$$

就是 $\mathbf{F}_{2^2}$ 中两两相异的三个 $\neq 0$ 的元素.

现在设 $p=3$, 考察 $\mathbf{Z}_3[x]$ 上的多项式

$$p(x)=x^2+1.$$

因为在 $\mathbf{Z}_3$ 中,

$$p(0)=1\neq 0,$$
$$p(1)=1+1=2\neq 0,$$
$$p(2)=2^2+1=2\odot 2+1=1+1=2\neq 0,$$

所以 $p(x)$ 在 $\mathbf{Z}_3$ 中没有根; 又因为 $p(x)$ 是二次的, 所以 $p(x)$ 是 $\mathbf{Z}_3[x]$ 中的不可约多项式. 根据上面的一般性讨论可知 $\mathbf{Z}_3[x]_{x^2+1}$ 是恰含 $3^2=9$ 个元素的有限域. 实际上,

$$\mathbf{Z}_3[x]_{x^2+1}$$
$$=\{0,\ 1,\ 2,\ x,\ x+1,\ x+2, 2x,\ 2x+1,\ 2x+2\}.$$

根据 $\mathbf{Z}_3[x]_{x^2+1}$ 中加法和乘法的定义, 容易写出 $\mathbf{Z}_3[x]_{x^2+1}$ 的加法表和乘法表:

$\oplus$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

$\odot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

在 $\mathbf{F}_{3^2}=\mathbf{J}_3[x]_{x^2+1}$ 中，任一 $\neq 0$ 的元素 α 均适合

$$\alpha^{3^2-1}=\alpha^8=1,$$

而对于 $\alpha=x+1,\ x+2,\ 2x+1,\ 2x+2$，则有

$$\alpha\neq 1,\ \alpha^2\neq 1,\ \alpha^3\neq 1,\ \cdots,\ \alpha^7\neq 1.$$

因此 $\mathbf{F}_{3^2}$ 中 $\neq 0$ 的元素，可表成它们之中任一个的幂次．譬如，

$$x+1,\ (x+1)^2,\ (x+1)^3,\ \cdots,\ (x+1)^7,\ (x+1)^8=1$$

就是 $\mathbf{F}_{3^2}$ 中两两相异的 8 个 $\neq 0$ 的元素．

今后我们将证明，$\mathbf{F}_{p^n}$ 中 $\neq 0$ 的元素 α 均适合条件

$$\alpha^{p^n-1}=1,$$

而 $\mathbf{F}_{p^n}$ 中至少有一个 $\neq 0$ 的元素 ξ 有性质

$$\xi\neq 1,\ \xi^2\neq 1,\ \xi^3\neq 1,\ \cdots,\ \xi^{p^n-2}\neq 1.$$

因此 $\mathbf{F}_{p^n}$ 中 $\neq 0$ 的元素都可以表成 ξ 的幂次，即

$$\xi,\ \xi^2,\ \xi^3,\ \cdots,\ \xi^{p^n-2},\ \xi^{p^n-1}=1$$

就是 $\mathbf{F}_{p^n}$ 中两两相异的 p^n-1 个 $\neq 0$ 的元素．

现在我们扼要地介绍一下域 F 上 n 个符号(或称文字) $x_1,\ x_2,\ \cdots,\ x_n$ 的多项式．形如

$$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$$

的式子，其中 $a\in F$ 而 $k_1,\ k_2,\ \cdots,\ k_n$ 都是非负整数，叫做系数

属于 F 的 n 个符号 $x_1, x_2, \cdots, x_n$ 的单项式，简称 F 上的 n 元单项式，而 $k_1+k_2+\cdots+k_n$ 就叫做它的次数．如果两个单项式中相同文字的幂次一样，它们就叫做同类项，有限个两两不是同类项的 F 上 n 元单项式的形式和

$$\sum_{k_1,k_2,\cdots,k_n} a_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

就叫做系数属于 F 的 n 个符号 $x_1, x_2, \cdots, x_n$ 的多项式，简称 F 上的 n 元多项式．一多项式中系数 $\neq 0$ 的单项式的最高次数就叫做这个多项式的次数．F 上的两个 n 元多项式叫做相等，或说它们是同一多项式，如果除去系数等于 0 的项以外，它们同类项的系数都相等．我们常用 $f(x_1, x_2, \cdots, x_n)$，$g(x_1, x_2, \cdots, x_n)$ 等符号来代表 F 上的 n 元多项式．F 上 n 元多项式的全体所组成的集合记作 $F[x_1, x_2, \cdots, x_n]$．可以象中学代数中一样，规定两个 n 元多项式

$$f(x_1, x_2, \cdots, x_n) = \sum_{k_1,k_2,\cdots,k_n} a_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n},$$

$$g(x_1, x_2, \cdots, x_n) = \sum_{k_1,k_2,\cdots,k_n} b_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

的和与积分别为

$$\begin{aligned} &f(x_1, x_2, \cdots, x_n) + g(x_1, x_2, \cdots, x_n) \\ &= \sum_{k_1,k_2,\cdots,k_n} (a_{k_1k_2\cdots k_n} + b_{k_1k_2\cdots k_n}) x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}, \end{aligned}$$

$$\begin{aligned} &f(x_1, x_2, \cdots, x_n) \cdot g(x_1, x_2, \cdots, x_n) \\ &= \sum_{k_1,k_2,\cdots,k_n} \sum_{l_1,l_2,\cdots,l_n} a_{k_1k_2\cdots k_n} b_{l_1l_2\cdots l_n} x_1^{k_1+l_1} x_2^{k_2+l_2} \cdots x_n^{k_n+l_n}. \end{aligned}$$

容易验证 $F[x_1, x_2, \cdots, x_n]$ 对于如上规定的加法运算和乘法运算是自封的．而且满足运算规则 I.1, I.2, I.3, I.4, II.1, I.2, II.3 和 III，但是 II.4 却不成立．

最后我们来引进域 F 上 n 个符号（或叫文字）$x_1, x_2, \cdots, x_n$ 的有理分式，为了书写简单起见，我们只讨论 $n=1$ 的情形，并把 x_1 记作 x．至于 $n>1$ 的情形，完全和 $n=1$ 的情形一样．

设 $a(x), b(x) \in F[x]$，而 $b(x) \neq 0$，那么式子

$$\frac{a(x)}{b(x)}$$

就叫 F 上符号 x 的一个有理分式，简称一元有理分式，更简称分式. $a(x)$ 叫做这个分式的分子，而 $b(x)$ 叫做它的分母，再设 $a_1(x), b_1(x) \in F[x]$，而 $b(x) \neq 0$. 我们把下面这两个分式

$$\frac{a(x)}{b(x)} \quad 和 \quad \frac{a_1(x)}{b_1(x)}$$

看作是同一个分式，或者说它们相等，并记作

$$\frac{a(x)}{b(x)} = \frac{a_1(x)}{b_1(x)},$$

如果
$$a(x)b_1(x) = b(x)a_1(x)$$

有理分式 $a(x)/b(x)$ 叫做真分式，如果 $\partial^0 a(x) < \partial^0 b(x)$；而有理分式 $a(x)/b(x)$ 叫做不可约分式，如果 $(a(x), b(x)) = 1$. 假定 $(a(x), b(x)) = d(x)$，那么可以设 $a(x) = a_1(x)d(x)$，$b(x) = b_1(x)d(x)$，而 $(a_1(x), b_1(x)) = 1$. 这时 $a_1(x)/b_1(x)$ 就是不可约因式而 $a(x)/b(x) = a_1(x)/b_1(x)$. 因此任一分式都等于一个不可约分式. 设 $a_1(x)/b_1(x)$ 和 $a_2(x)/b_2(x)$ 都是不可约因式，如果 $a_1(x)/b_1(x) = a_2(x)/b_2(x)$，那么 $a_1(x)b_2(x) = b_1(x)a_2(x)$；因 $(a_1(x), b_1(x)) = (a_2(x), b_2(x)) = 1$，根据唯一因式分解定理就一定有 $a_1(x) = ca_2(x)$，$b_1(x) = cb_2(x)$，这里 $c \in F$ 而 $c \neq 0$. 如果更假定 $b_1(x)$ 和 $b_2(x)$ 的首项系数都等于 e，那么就一定有 $b_1(x) = b_2(x)$，$a_1(x) = a_2(x)$. 因此任一分式都等于唯一的一个分母的首项系数等于 1 的不可约因式.

F 上一个符号 x 的有理分式的全体所组成的集合记作 $F(x)$. 下面我们来规定 $F(x)$ 中的加法运算和乘法运算. 设

$$\frac{a(x)}{b(x)} \quad 和 \quad \frac{c(x)}{d(x)}$$

是 $F(x)$ 中任意两个元素，即 $a(x)$，$b(x)$，$c(x)$，$d(x)$ 都是 $F[x]$ 中的元素，而 $b(x)\neq 0$，$d(x)\neq 0$. 我们按下面这两个式子来规定它们的和与积：

$$\frac{a(x)}{b(x)}+\frac{c(x)}{d(x)}=\frac{a(x)\cdot d(x)+b(x)\cdot c(x)}{b(x)\cdot d(x)}, \tag{10}$$

$$\frac{a(x)}{b(x)}\cdot\frac{c(x)}{d(x)}=\frac{a(x)\cdot c(x)}{b(x)\cdot d(x)}, \tag{11}$$

不难验证，如果

$$\frac{a(x)}{b(x)}=\frac{a_1(x)}{b_1(x)},\quad \frac{c(x)}{d(x)}=\frac{c_1(x)}{d_1(x)},$$

那么一定有

$$\frac{a(x)}{b(x)}+\frac{c(x)}{d(x)}=\frac{a_1(x)}{b_1(x)}+\frac{c_1(x)}{d_1(x)}, \tag{12}$$

$$\frac{a(x)}{b(x)}\cdot\frac{c(x)}{d(x)}=\frac{a_1(x)}{b_1(x)}\cdot\frac{c_1(x)}{d_1(x)} \tag{13}$$

举(12)式为例，根据(10)式，有

$$\frac{a(x)}{b(x)}+\frac{c(x)}{d(x)}=\frac{a(x)\cdot d(x)+b(x)\cdot c(x)}{b(x)\cdot d(x)},$$

$$\frac{a_1(x)}{b_1(x)}+\frac{c_1(x)}{d_1(x)}=\frac{a_1(x)d_1(x)+b_1(x)\cdot c_1(x)}{b_1(x)\cdot d_1(x)}.$$

但是

$$\begin{aligned}&[a(x)\cdot d(x)+b(x)c(x)][b_1(x)d_1(x)]\\&=a(x)\cdot b_1(x)d(x)d_1(x)+b(x)b_1(x)c(x)d_1(x)\\&=b(x)a_1(x)d(x)d_1(x)+b(x)b_1(x)d(x)c_1(x)\\&=[b(x)d(x)][a_1(x)d_1(x)+b_1(x)c_1(x)]\end{aligned}$$

由此就推出(12)式. 同样可证(13)式成立. 这样，按(10)，(11)两式分别定义的 $F(x)$ 中的加法运算和乘法运算是合理的. 更进一步还可以验证，$F(x)$对于按(10)，(11)两式分别定义的加法运算和乘法运算来说是一个域，以 $\frac{0}{e}$ 为零元素，以 $\frac{e}{e}$ 为单位元素，而 $F(x)$ 中一个非零元素 $a(x)/b(x)$ 的逆

元素是 $b(x)/a(x)$. 我们把这些验证都留给读者作为练习. 这样我们又得到一个域的例子. 我们把 $F(x)$ 这个域叫做域 F 上一个符号 x 的有理分式域,简称一元有理分式域,我们还把 $F[x]$ 中的元素 $a(x)$ 与 $F(x)$ 中的元素 $a(x)/e$ 看成同一个元素. 这样,就把 $F[x]$ 看成 $F(x)$ 的子集,特别 F 就是 $F(x)$ 的子域,而 F 的零元素和单位元素就分别是 $F(x)$ 的零元素和单位元素.

§3 域的特征和素域

在前面两节里我们见到, $\mathbf{Q}$, $\mathbf{R}$ 和 $\mathbf{C}$ 这一类域与 $\mathbf{Z}_p$ 和 $\mathbf{F}_{p^n}$ 这一类域有一点很不一样. 这就是: 对于前者来说, 任意有限个 1 的和都不等于 0; 而对于后者来说, p 个 1 的和都等于 0. 因此, 为了区别这两类域, 在任意域 F 中, 考察 F 的单位元素 e, 两个 e 的和 $2e$, 3 个 e 的和 $3e$, … 这一系列元素:

$$e,\ 2e,\ 3e,\ \cdots \tag{1}$$

是有益处的. 首先,我们给出下面的定义

定义 1 设 F 是任意一域, 而 e 是它的单位元素. 如果对于任意正整数 m, 我们都有 $me\neq 0$, 我们就说 F 的特征是 0, 或 F 是特征 0 的域. 如果有正整数 m 存在使 $me=0$, 那么就说 F 的特征不等于 0, 而适合条件 $pe=0$ 的最小正整数 p 就叫做 F 的特征, 或者说 F 是特征 p 的域.

我们先来证明

定理 1 设 F 是任意一域, 那么 F 的特征或者是 0, 或者是一个素数 p.

证. 设 F 的特征不等于 0, 即有正整数 m 存在使 $me=0$. 我们要证明, 适合条件 $pe=0$ 的最小正整数 p 一定是一个素

数. 我们用反证法来证明. 如果 p 不是素数, 那么 p 有分解 $p=p_1p_2$ 而 $1<p_1,\ p_2<p$. 于是

$$pe=(p_1p_2)e=0.$$

因 $e^2=e$, 所以有

$$(p_1e)(p_2e)=(p_1p_2)e.$$

因此 $$p_1e=0 \quad 或 \quad p_2e=0.$$

但 $1<p_1,\ p_2<p$, 这与 p 的最小性相矛盾. 因此 p 一定是素数.

注意, **Q**, **R** 和 **C** 都是特征 0 的域, 而 $\mathbf{Z}_p$ 和 $\mathbf{F}_{p^n}$ 都是特征 p 的域.

更进一步,我们有

定理 2 设 F 是任意一域. 如果 F 是特征 0 的域,那么对于 F 中任意一个不等于 0 的元素 a 和任意正整数 m, 都有 $ma\neq 0$, 而且

$$0,\ \pm a,\ \pm 2a,\ \pm 3a,\ \cdots \tag{2}$$

这一系列元素两两相异. 如果 F 是特征 p 的域, 那么对于 F 中任意一个不等于 0 的元素 a 都有 $pa=0$, p 是适合条件 $pa=0$ 的最小正整数,而且

$$0,\ a,\ 2a,\ 3a,\ \cdots,\ (p-1)a \tag{3}$$

这 p 个元素两两相异. 更进一步, 设 m 是整数, 那么 $ma=0$, 当且仅当 $p|m$.

证. 先设 F 是特征 0 的域. 如果对于 F 中的某一个 $\neq 0$ 的元素 a 有正整数 m 存在使 $ma=0$, 那么

$$a(me)=m(ae)=ma=0.$$

但是 $a\neq 0$, 因此一定有 $me=0$, 这与 F 的特征是 0 相矛盾. 所以对于 F 中任意一个 $\neq 0$ 的元素 a 和任意正整数 m, 一定都有 $ma\neq 0$. 其次, 如果(2)中有两个元素相等, 譬如 $ka=la$ 而 $k<l$, 那么

$$(l-k)a=la-ka=0.$$

但是 $l-k>0$, 所以这是不可能的.

再设 F 的特征是 p, 那么 $pe=0$. 设 a 是 F 中任意一个 $\neq 0$ 的元素,那么

$$pa=p(ea)=(pe)a=0\cdot a=0.$$

又如果 m 是具有性质 $ma=0$ 的正整数,那么

$$(me)a=m(ea)=ma=0,$$

但是 $a\neq 0$, 所以 $me=0$. 根据域的特征的定义, p 是适合条件 $pe=0$ 的最小正整数, 所以一定有 $p\leqslant m$. 因此 p 是适合条件 $pa=0$ 的最小正整数. 其次, 如果(3)中有两个元素相等, 譬如 $ka=la$ 而 $0\leqslant k<l<p$, 那么

$$(l-k)a=la-ka=0.$$

但是 $0<l-k<p$, 这与 p 是适合条件 $pa=0$ 的最小正整数这一事实相矛盾.

最后我们证明, 当 F 是特征 p 的域时, 设 a 是 F 中任意一个不等于 0 的元素而 m 是整数, 那么 $ma=0$ 当且仅当 $p|m$. 首先, 如果 $p|m$, 即 $m=qp$ 而 q 是个整数, 那么

$$ma=(qp)a=q(pa)=q\cdot 0=0.$$

反之, 设 $ma=0$. 如果 $p\nmid m$, 那么 $(p, m)=1$. 于是有整数 c 和 d 存在使

$$1=cp+dm$$

因此 $$a=1\cdot a=(cp+dm)a=(cp)a+(dm)a$$
$$=c(pa)+d(ma)=c\cdot 0+d\cdot 0=0+0=0.$$

这是不可能的,因此一定有 $p|m$.

于是定理 2 就完全证明了.

我们先来考察特征 p 的域. 设 F 是特征 p 的任意域, e 是它的单位元素. 令

$$\Pi=\{0, e, 2e, \cdots, (p-1)e\}.$$

因 $pe=0$, 所以对任意整数 k, $(kp)e=k(pe)=k\cdot 0=0$. 因此 Π 中任意两个元素 ke 和 le 的和与积可以按照下面的公式进行计算:

$$ke+le=(k+l)_p e,$$
$$ke\cdot le=(kl)_p e.$$

这就是说, Π 对于 F 中的加法运算和乘法运算来说是自封的. 又 F 的零元素 0 和单位元素 e 都在 Π 中. 显然 Π 中任一元素 ke 的负元素 $(p-k)e$ 也属于 Π. 更进一步, 仿照§1例4中关于 $\mathbf{Z}_p$ 中任一 $\neq 0$ 的元素都有逆元素存在的证明, 可证 Π 中任一 $\neq 0$ 元素的逆元素一定属于 Π. 这就证明了 Π 是 F 的子域.

更进一步, 因为 F 的任一子域都含有 F 的单位元素 e, 因而也含有 $2e, 3e, \cdots, (p-1)e$, 所以一定包有 Π. 这就是说, Π 是 F 的最小的子域. 我们把 Π 叫做 F 的**素域**.

与§1例4中的 $\mathbf{Z}_p$ 相比较, 可以发现从 Π 到 $\mathbf{Z}_p$ 的映射

$$ke\to k \quad (0\leqslant k<p)$$

是从 Π 到 $\mathbf{Z}_p$ 的一一对应, 而且这个映射将 Π 中任意两个元素 ke 与 le 的和 $ke+le$ 映到 ke 的象 k 与 le 的象 l 在 $\mathbf{Z}_p$ 中的和 $k\oplus l$, 并把 ke 与 le 积 $ke\cdot le$ 映到 ke 的象 k 与 le 的象 l 在 $\mathbf{Z}_p$ 中的积 $k\odot l$. 这时我们说 Π 和 $\mathbf{Z}_p$ 是**同构的**.

我们给出下面这个一般性的定义.

定义 2 设 F 和 F' 是两个域. 如果可以在 F 和 F' 的元素之间建立一个一一对应

$$\sigma: a\to\sigma(a) \quad (a\in F,\ \sigma(a)\in F'),$$

而且这个一一对应保持域的加法运算与乘法运算, 这就是说, F 中任意两个元素 a 与 b 的和 $a+b$ 对应到 a 的象 $\sigma(a)$ 与 b 的象 $\sigma(b)$ 在 F' 中的和 $\sigma(a)+\sigma(b)$, 而 a 与 b 的积 ab 对应到 $\sigma(a)$ 与 $\sigma(b)$ 的积 $\sigma(a)\sigma(b)$, 也就是说, 如果这个一一对

应 σ 适合条件：对任意 $a, b\in F$,

$$\sigma(a+b)=\sigma(a)+\sigma(b),$$
$$\sigma(ab)=\sigma(a)\sigma(b),$$

我们就说 F 和 F' 同构，而 σ 是从 F 到 F' 的一个同构映射或同构对应或简称同构.

同构的域只不过是它们相应的元素的符号不同而已. 因此今后我们往往把同构的域看成是同一个域.

我们再来考察特征 0 的域. 设 F 是特征 0 的任意域, e 是它的单位元素，那么根据定理 2, 下面这一系列元素

$$\cdots,\ -2e,\ -e,\ 0,\ e,\ 2e,\ \cdots \tag{4}$$

两两相异. 当 $n\neq 0$ 时，将 ne 的逆元素记作 $(ne)^{-1}$. 令

$$\Pi=\{(me)(ne)^{-1}\mid m,\ n\in\mathbf{Z},\ n\neq 0\},$$

那么 $$(me)(ne)^{-1}=(m'e)(n'e)^{-1},$$

当且仅当 $$mn'=nm',$$

不难验证

$$(me)(ne)^{-1}+(m'e)(n'e)^{-1}=[(mn'+nm')e][(nn')e]^{-1},$$
$$(me)(ne)^{-1}\cdot(m'e)(n'e)^{-1}=[(mm')e][(nn')e]^{-1}.$$

因此 Π 对于 F 中的加法运算和乘法运算都是自封的. 又 F 中的零元素 0 和单位元素 e 都在 Π 中. 再任取 Π 中一元素 $(me)(ne)^{-1}$, 那么 $(-me)(ne)^{-1}$ 也属于 Π, 而

$$(me)(ne)^{-1}+(-me)(ne)^{-1}=0$$

当 $m\neq 0$ 时，即当 $(me)(ne)^{-1}\neq 0$ 时，$(ne)(me)^{-1}$ 也属于 Π, 而

$$(me)(ne)^{-1}\cdot(ne)(me)^{-1}=e.$$

这证明了 Π 是 F 的子域.

更进一步，因为 F 的任一子域都含有 F 的单位元素 e, 因而也含有(4)中每一个元素，所以也含有每一个形状是

$$(me)(ne)^{-1}\quad(m,\ n\in\mathbf{Z},\ n\neq 0)$$

的元素，即 F 一定包有 Π. 这就是说，Π 是 F 的最小的子域. 我们把 Π 叫做 F 的素域.

与有理数域 $\mathbf{Q}$ 相比较：我们知道每个有理数都可以表成形状

$$\frac{m}{n}(m,\ n\in\mathbf{Z},\ n\neq 0),$$

即
$$\mathbf{Q}=\left\{\frac{m}{n}\middle|\, m,\ n\in\mathbf{Z},\ n\neq 0\right\}.$$

而且
$$\frac{m}{n}=\frac{m'}{n'},$$

当且仅当
$$mn'=nm'.$$

可以发现从 Π 到 $\mathbf{Q}$ 的映射

$$(me)(ne)^{-1}\to\frac{m}{n}$$

是从 Π 到 $\mathbf{Q}$ 的一一对应，而且这个映射将 Π 中任意两个元素 $(me)(ne)^{-1}$ 与 $(m'e)(n'e)^{-1}$ 的和 $[(mn'+nm')e][(nn')e]^{-1}$ 映到 $(me)(ne)^{-1}$ 的象 $\frac{m}{n}$ 与 $(m'e)(n'e)^{-1}$ 的象 $\frac{m'}{n'}$ 的和 $\frac{mn'+nm'}{nn'}$，并把 $(me)(ne)^{-1}$ 与 $(m'e)(n'e)^{-1}$ 的积 $[(mm')e]\cdot[(nn')e]^{-1}$ 映到 $\frac{m}{n}$ 与 $\frac{m'}{n'}$ 的积 $\frac{mm'}{nn'}$. 因此这时 Π 与 $\mathbf{Q}$ 同构.

综合上面的讨论，我们有

定理 3 设 F 是任意域，用 Π 表示 F 的素域(即 F 的最小子域)，那么当 F 的特征是一个素数 p 时，Π 就与 $\mathbf{Z}_p$ 同构；而当 F 的特征是 0 时，Π 就与 $\mathbf{Q}$ 同构.

系理 如果 F 是有限域，那么 F 的特征一定不等于 0.

证. 如果 F 的特征是 0，那么 F 的素域 Π 就与有理数域 $\mathbf{Q}$ 同构. 但 $\mathbf{Q}$ 是个无限域，因此这时 F 也是无限域. 这样就引出矛盾.

关于同构的域，我们还有下面这个结果.

定理 4 设 F 和 F' 是两个同构的域，而

$$\sigma: a \to \sigma(a)\ (a \in F,\ \sigma(a) \in F')$$

是从 F 到 F' 的一个同构对应，那么在这个同构对应之下，F 的零元素一定映到 F' 的零元素，而 F 的单位元素一定映到 F' 的单位元素．更进一步，设 F 中的元素 a 映到 F' 中的元素 $\sigma(a)$，那么 a 的负元素 $-a$ 一定映到 $\sigma(a)$ 的负元素 $-\sigma(a)$，而当 $a \neq 0$ 时，a 的逆元素 a^{-1} 一定映到 $\sigma(a)$ 的逆元素 $\sigma(a)^{-1}$.

证．设 0 和 e 分别是 F 的零元素和单位元素．我们来证明 $\sigma(0)$ 和 $\sigma(e)$ 分别是 F' 的零元素和单位元素．我们有

$$a+0=a, \quad 对任意\ a \in F.$$

因此
$$\sigma(a)+\sigma(0)=\sigma(a+0)=\sigma(a).$$

因 σ 是一一对应，所以当 a 遍历 F 时，$\sigma(a)$ 必遍历 F'，这就是说，上式中的 $\sigma(a)$ 可以是 F' 中的任一元素．这证明了 $\sigma(0)$ 是 F' 的零元素．同理可证，$\sigma(e)$ 是 F' 的单位元素.

更进一步，对任意 $a \in F$，我们有

$$\sigma(a)+\sigma(-a)=\sigma(a+(-a))=\sigma(0).$$

但另一方面，又有

$$\sigma(a)+(-\sigma(a))=\sigma(0),$$

因此有
$$\sigma(a)+\sigma(-a)=\sigma(a)+(-\sigma(a)),$$

那么，利用加法消去律推出

$$\sigma(-a)=-\sigma(a).$$

同理可证，当 $a \neq 0$ 时，

$$\sigma(a^{-1})=\sigma(a)^{-1}.$$

系理 1 设 F 和 F' 是两个同构的域，而

$$\sigma: a \to \sigma(a)$$

是从 F 到 F' 的一个同构对应，那么

$$\sigma(a-b)=\sigma(a)-\sigma(b), \quad 对任意\ a,\ b \in F,$$

$$\sigma(ab^{-1})=\sigma(a)\sigma(b)^{-1},\quad 对任意 a,\ b\in F,\ 而 b\neq 0.$$

证. 对任意 $a,\ b\in F$, 我们有

$$\sigma(a-b)=\sigma(a+(-b))=\sigma(a)+\sigma(-b)=\sigma(a)-\sigma(b).$$

又如果 $b\neq 0$, 那么

$$\sigma(ab^{-1})=\sigma(a)\sigma(b^{-1})=\sigma(a)\sigma(b)^{-1}.$$

系理 2 设 F 和 F' 是两个同构的域, 那么 F 和 F' 的特征一定相等.

证. 设

$$\sigma: a\to\sigma(a)$$

是从 F 到 F' 的一个同构对应. 根据定理 4, F 的单位元素 e 在 σ 之下的象 $\sigma(e)$ 就是 F' 的单位元素. 那么对于任意正整数 m,

$$\sigma(me)=\sigma(\underbrace{e+e+\cdots+e}_{m\text{个}})$$
$$=\underbrace{\sigma(e)+\sigma(e)+\cdots+\sigma(e)}_{m\text{个}}=m\sigma(e),$$

即 me 在 σ 之下的象是 $m\sigma(e)$.

如果 F 的特征是 0, 那么 $me\neq 0$, 对任意正整数 m. 但根据定理 4, F 的零元素 0 在 σ 之下的象 $\sigma(0)$ 是 F' 的零元素, 因此 $m\sigma(e)\neq\sigma(0)$, 即 F' 的特征也是 0.

如果 F' 的特征是 p, p 是一个素数, 那么 $pe=0$, 因此 $p\sigma(e)=\sigma(0)$, 于是 F' 的特征 $\neq 0$. 设 F' 的特征是 p', 而 p' 是一个素数, 那么 $p'|p$. 因 p 也是素数, 所以 $p'=p$.

从系理 2 可以知道, 域的特征的确是域的一个特征性质.

例 我们来证明, 仅含 4 个元素的域一定与 §2 中所构造的 $\mathbf{Z}_2[x]_{x^2+x+1}$ 同构.

设 $\mathbf{F}_4$ 是仅含 4 个元素的一个域. 根据定理 3 的系理, $\mathbf{F}_4$ 的特征一定是一个素数 p. 设 e 是 $\mathbf{F}_4$ 的单位元素. 根据定理

3, $\mathbf{F}_4$ 的素域

$$\Pi=\{0,\ e,\ 2e,\ \cdots,\ (p-1)e\}$$

就是含 p 个元素的域，而且与 $\mathbf{Z}_p$ 同构，但 $\mathbf{F}_4$ 仅含 4 个元素，因此 $p\leqslant 3$.

我们先证明 $p\neq 3$. 假定 $p=3$, 那么 Π 是含 3 个元素 0, e, $2e$ 的域. 因此 $\mathbf{F}_4$ 一定有一个元素不属于 Π. 将这个元素记作 a. 于是

$$\mathbf{F}_4=\{0,\ e,\ 2e,\ a\}.$$

但是 $\mathbf{F}_4$ 对于加法运算自封，因此 $a+e\in\mathbf{F}_4$. 如果 $a+e=0$, 则 $a=2e$; 如果 $a+e=e$, 则 $a=0$; 如果 $a+e=2e$, 则 $a=e$; 如果 $a+e=a$, 则 $e=0$; 这都是不可能的. 这证明了 $p\neq 3$. 因此一定有 $p=2$, 即

$$\Pi=\{0,\ e\},$$

而 Π 与 $\mathbf{Z}_2$ 同构.

现在设 y 是 $\mathbf{F}_4$ 中的一个不属于 Π 的元素，那么 $y+e\neq 0$, e, y. 于是

$$\mathbf{F}_4=\{0,\ e,\ y,\ y+e\}.$$

因 $\mathbf{F}_4$ 对于乘法运算自封，所以 $y^2\in\mathbf{F}_4$. 显然 $y^2\neq 0$. 如果 $y^2=e$, 那么 $(y-e)^2=0$, 于是 $y=e$, 这是不可能的; 如果 $y^2=y$, 那么利用乘法消去律也有 $y=e$. 因此，一定有 $y^2=y+e$, 即

$$y^2+y+e=0.$$

那么可以算出 $\mathbf{F}_4$ 的加法表与乘法表如下:

$+$	0	e	y	$y+e$
0	0	e	y	$y+e$
e	e	0	$y+e$	y
y	y	$y+e$	0	e
$y+e$	$y+e$	y	e	0

$\cdot$	0	e	y	$y+e$
0	0	0	0	0
e	0	e	y	$y+e$
y	0	y	$y+e$	e
$y+e$	0	$y+e$	e	y

将 $\mathbf{F}_4$ 的加法表与乘法表和 §2 中写出的 $\mathbf{Z}_2[x]_{x^2+x+1}$ 的加法表与乘法表相比较，可知从 $\mathbf{F}_4$ 到 $\mathbf{Z}_2[x]_{x^2+x+1}$ 的一一对应

$$0\to 0,\quad e\to 1,\quad y\to x,\quad y+e\to x+1$$

是 $\mathbf{F}_4$ 与 $\mathbf{Z}_2[x]_{x^2+x+1}$ 之间的同构对应. 因此 $\mathbf{F}_4$ 与 $\mathbf{Z}_2[x]_{x^2+x+1}$ 同构.

今后我们将证明，如果两个有限域的元素个数相等，那么它们一定同构.

我们再指出，从上面算出的仅含 4 个元素的有限域 $\mathbf{F}_4$ 的加法表和乘法表可以看出，从 $\mathbf{F}_4$ 到它自身之上的一一对应

$$0\to 0,\quad e\to e,\quad y\to y+e,\quad y+e\to y$$

是从 $\mathbf{F}_4$ 到它自身的同构对应，我们把它叫做 $\mathbf{F}_4$ 的一个自同构.

一般地，我们有下面这个定义

定义 3 设 F 是一个域. 那么从 F 到它自身的同构对应叫做 F 的自同构.

显然，将 F 中任一元素都映到它自己的映射

$$a\to a,\quad 对一切\ a\in F$$

(这个映射叫做恒同映射)是 F 的一个自同构. 这个自同构叫做恒同自同构.

最后我们证明下面这个在特征 p 的域里所特有的运算规则.

定理 5 设 F 是特征 p 的域，而 a 和 b 是 F 中任意两个元素，那么一定有

$$(a+b)^p=a^p+b^p.$$

证. 根据二项式定理，我们有

$$(a+b)^p=\sum_{i=0}^{p}\binom{p}{i}a^ib^{p-i}.$$

因 $$\binom{p}{i}=\frac{p!}{i!(p-i)!}$$

是 p 中取 i 的组合数，所以一定是个整数．显然 $p|p!$．又因 p 是素数，所以当 $0<i<p$ 时，一定有 $p\nmid i!$ 和 $p\nmid(p-i)!$，因此 $p\nmid i!(p-i)!$．所以，当 $0<i<p$ 时，

$$p\left|\binom{p}{i}\right..$$

那么根据定理 2，当 $0<i<p$ 时，一定有

$$\binom{p}{i}a^ib^{p-i}=0.$$

因此有 $$(a+b)^p=a^p+b^p.$$

系理 1 设 F 是特征 p 的域，而 a 和 b 是 F 中任意两个元素，那么一定有

$$(a-b)^p=a^p-b^p.$$

证．根据定理 5，我们有

$$\begin{aligned}(a-b)^p&=(a+(-b))^p=a^p+(-b)^p\\&=a^p+((-1)b)^p=a^p+(-1)^pb^p.\end{aligned}$$

当 $p>2$ 时，p 是奇数，我们有 $(-1)^p=-1$．因此

$$(a-b)^p=a^p-b^p.$$

当 $p=2$ 时，$2a=0$，对任意 $a\in F$．因此 $a=-a$，对任意 $a\in F$．所以也有

$$(a-b)^2=a^2+b^2=a^2-b^2.$$

系理 2 设 F 是特征 p 的域，而 $a_1, a_2, \cdots, a_m$ 是 F 中任意 m 个元素，那么一定有

$$(a_1+a_2+\cdots+a_m)^p=a_1^p+a_2^p+\cdots+a_m^p.$$

证．对 m 用数学归纳法即可证明本系理，细节请读者自行补出．

系理 3 设 F 是特征 p 的域，a 和 b 是 F 中任意两个元素，而 n 是任意非负整数，那么一定有

$$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}.$$

证. 对 n 用数学归纳法即可证明本系理，细节请读者自己补出.

系理 4 设 F 是个有限域，它的特征是 p，而 n 是任意非负整数，那么从 F 到它自身的映射

$$\sigma_n: a\to a^{p^n}(a\in F)$$

是 F 的一个自同构.

证. 首先证明 σ_n 是个一一对应. 设 $\sigma_n(a)=\sigma_n(b)$，即 $a^{p^n}=b^{p^n}$. 那么根据系理 3 有 $(a-b)^{p^n}=a^{p^n}-b^{p^n}=0$. 那么从 § 1 定理 2 的 iv) 推出 $a-b=0$. 因此 $a=b$. 这就是说，当 $a\neq b$ 时，一定有 $\sigma_n(a)\neq\sigma_n(b)$. 因此 σ_n 是一对一的，又因 F 的元素个数有限，所以 σ_n 也是映上的. 因此 σ_n 是从 F 到 F 的一个一一对应.

其次，根据系理 3，我们有

$$(a+b)^{p^n}=a^{p^n}+b^{p^n}.$$

因此 $$\sigma_n(a+b)=\sigma_n(a)+\sigma_n(b).$$

又根据乘法交换律，我们有

$$(ab)^{p^n}=a^{p^n}b^{p^n}.$$

因此 $$\sigma_n(ab)=\sigma_n(a)\sigma_n(b).$$

这证明了 σ_n 是 F 的一个自同构.

在上面所举的例子中，$\mathbf{F}_4$ 的自同构

$$0\to 0,\quad e\to e,\quad y\to y+e,\quad y+e\to y$$

实际上就是自同构

$$a\to a^2(a\in\mathbf{F}_4).$$

§4 有限域的乘法群

前面我们已经说过，在域的公理中，I 是关于加法的，II 是关于乘法的，而且它们是平行的. 如果说有不同的话，就只是在 II.3 中要求 $e\neq 0$，而 II.4 则是对域中 $\neq 0$ 的元素说的. 但是如果我们用 F^* 来代表 F 中全体 $\neq 0$ 的元素所组成的集合，那么根据 §1 定理 2 中的 iv)，域的乘法运算对于 F^* 来说是自封的，而且满足以下运算规则:

1) 对任意 $a, b\in F^*$，有

$$a\cdot b=b\cdot a.$$

2) 对任意 $a, b, c\in F^*$，有

$$(a\cdot b)\cdot c=a\cdot(b\cdot c).$$

3) F^* 中有一个元素，把它记作 e，具有性质

$$a\cdot e=a,\quad 对一切\ a\in F^*.$$

4) 对任意 $a\in F^*$，F^* 中有一个元素，把它记作 a^{-1}，具有性质

$$a\cdot a^{-1}=e.$$

(应该提醒一下，4) 的成立用到了 §1 定理 2 的系理 2!) 这样一来，F^* 中乘法运算所满足的运算规则就与 F 中加法运算所满足的运算规则形式上完全一样，所不同的只不过是运算符号不同而已，即前者是"·"，而后者是"+". 这样我们就归纳出交换群的概念.

定义 1 设 G 是一个非空集合. 假定在 G 中规定了一种运算，通常叫做乘法运算，即对于 G 中任意两个元素 a 和 b，可以对它们进行乘法运算，把运算的结果记作 $a\cdot b$，叫做它们的积. 我们还要求 G 中任意两个元素经乘法运算的结果即它们的积，仍是 G 中的元素，这就是说，G 对于乘法运算是自

封的. 我们说 G 对于所规定的乘法运算是一个交换群，如果以下运算规则成立:

1) 对任意 $a, b\in G$, 有

$$a\cdot b=b\cdot a. \qquad \text{(交换律)}$$

2) 对任意 $a, b, c\in G$, 有

$$(a\cdot b)\cdot c=a\cdot(b\cdot c). \qquad \text{(结合律)}$$

3) G 中有一个元素,把它记作 e, 具有性质

$$a\cdot e=a, \quad 对一切 a\in G.$$

4) 对任意 $a\in G$, G 中有一个元素，把它记作 a^{-1}, 具有性质

$$a\cdot a^{-1}=e.$$

我们往往把定义 1 中的 1), 2), 3), 4) 叫做交换群的公理. 我们从交换群的公理出发,先来推导下面这个定理.

定理 1 设 G 是任意一个交换群,那么

i) G 中适合条件

$$a\cdot e=a, \quad 对一切 a\in G$$

的元素 e 是唯一确定的.

ii) 对任意 $a\in G$, G 中适合条件

$$a\cdot a^{-1}=e$$

的元素 a^{-1} 是唯一确定的.

证. 设 G 中有元素 e 和 e' 分别适合条件

$$a\cdot e=a, \quad 对一切 a\in G,$$

$$a\cdot e'=a, \quad 对一切 a\in G.$$

在前一式中令 $a=e'$, 有

$$e'\cdot e=e'.$$

在后一式中令 $a=e$, 有

$$e\cdot e'=e.$$

但是根据 1), 有

$$e'\cdot e=e\cdot e',$$

因此一定有 $$e=e'.$$

这证明了 i) 成立。

其次，对任意 $a\in G$，设 G 中有 a^{-1} 和 b 有性质

$$a\cdot a^{-1}=e,$$

$$a\cdot b=e.$$

那么 $$b=b\cdot e=b\cdot(a\cdot a^{-1})=(b\cdot a)\cdot a^{-1}$$
$$=(a\cdot b)a^{-1}=e\cdot a^{-1}=a^{-1}\cdot e=a^{-1}.$$

这证明了 ii) 成立.

基于定理1，我们给出下面这个定义.

定义 2 设 G 是任意一个交换群，G 中适合条件

$$a\cdot e=a,\quad 对一切\ a\in G$$

的唯一的那个元素 e 叫做 G 的*单位元素*. 对任意 $a\in G$，G 中适合条件

$$a\cdot a^{-1}=e$$

的唯一的那个元素 a^{-1} 叫做 a 的*逆元素*.

有时我们也把交换群 G 中的运算记作"+"，叫做*加法运算*，并把 G 中两个元素 a 与 b 经加法运算的结果记作 $a+b$，叫做 a 与 b 的*和*. 这时就要把群的公理中的运算符号改成"+"；把 3) 中的 e 改记成 0，有时也把它叫做 G 的*零元素*；把 4) 中的 a^{-1} 改记成 $-a$，有时也把它叫做 a 的*负元素*.

显然，任意一域 F 中的全体元素所组成的集合对于 F 中的加法运算来说是一个交换群；这个交换群叫做域 F 的*加法群*. 又根据本节开始时的分析，我们知道，域 F 中全体 $\neq 0$ 的元素所组成的集合对于 F 中的乘法运算来说也是一个交换群；这个交换群叫做域 F 的*乘法群*，并用符号 F^* 来代表它. 反过来，我们有

定理 2 设 F 是一个非空集合. 假定在 F 中规定了加法

(记作"+")和乘法(记作"·")两种运算，并假定 F 对于这两种运算都是自封的．如果以下条件成立：

I′ F 对于加法运算来说是一个交换群，并把这个交换群的单位元素记作 0，

II′ F 中全体 $\neq 0$ 的元素所组成的集合 F^* 对于 F 中规定的乘法运算来说也是一个交换群，

III′ 对任意 $a, b, c \in F$，有

$$a(b+c)=ab+ac.$$

那么 F 就是一个域．

证．问题是要证明从 I′, II′, III′ 可导出 I, II, III．注意 I′ 只不过是 I 利用交换群的概念的另一表达方法，而 III′ 与 III 完全一样．因此 I 和 III 成立．再注意，II.4 显然包含在 II′ 中．因此只要证明 II.1, II.2, II.3 成立即可．

我们先证明

$$0\cdot a=a\cdot 0=0, \quad 对任意 a\in F. \tag{1}$$

根据 I.3 和 III，我们有

$$0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a,$$

用 b 表 $0\cdot a$ 在 F 的加法群中的负元素，根据 I.4 可知 b 是存在的．那么

$$\begin{aligned}0\cdot a&=0\cdot a+0=0\cdot a+(0\cdot a+b)\\&=(0\cdot a+0\cdot a)+b=0\cdot a+b=0.\end{aligned}$$

同理可证的 $a\cdot 0=0$．

用 e 表 F^* 对于乘法来说所组成的交换群的单位元素，那么自然有 $a\cdot e=a$，对一切 $a\in F^*$．又在(1)中取 $a=e$，就有 $0\cdot e=0$，因此 $a\cdot e=a$，对一切 $a\in F$．这证明了 II.3 成立．

II.1 和 II.2 显然对于 F^* 中的任意三个 $\neq 0$ 的元素 a, b, c 均成立．如果 a, b 中有等于 0 的，那么利用(1)可推出 $a\cdot b=b\cdot a$ 的双方都等于 0．因此 II.1 对于 F 中任意两个元素 a, b

都成立. 同理可证II.2对F中任意三个元素a, b, c都成立.

这证明了F中加法运算和乘法运算满足运算规则I, II, III. 因此F是域.

我们也往往把I′, II′, III′叫做域的公理. 值得注意的是,引进了交换群的概念之后,域的公理简洁得多.

我们这里顺便提一下,群是抽象代数的基本概念之一,有着许多极为重要的应用. 在定义1中把运算规则1)取消,我们就得到群的定义. 但在本书中,我们只讨论交换群.

我们再举几个交换群的例子, 这几个例子对于编码来说是重要的.

例1 设m是个正整数,令

$$\mathbf{Z}_m=\{0, 1, 2, \cdots, m-1\}.$$

在§1中, 我们曾在$\mathbf{Z}_m$中如下地规定了乘法运算, 即模m乘法运算

$$a\odot b=(a\cdot b)_m, \quad \text{对任意 } a, b\in\mathbf{Z}_m.$$

显然$\mathbf{Z}_m$对于如上规定的乘法运算是自封的, 而且利用§1中关于$\mathbf{Z}_p$是域的有关证明可证$\mathbf{Z}_m$中的乘法运算满足运算规则1), 2), 3),但要注意

$$a\odot 1=a, \quad \text{对任意 } a\in\mathbf{Z}_m.$$

可是运算规则4)却不成立. 实际上,$0\odot a=0$,对任意$a\in\mathbf{Z}_m$,因此在$\mathbf{Z}_m$中0没有逆元素. 所以$\mathbf{Z}_m$对于上面规定的乘法运算不成交换群. 不但如此, 当m是复合数时, 从$\mathbf{Z}_m$中除去0之后所得的集合

$$\mathbf{Z}_m\backslash\{0\}=\{1, 2, 3, \cdots, m-1\}$$

对于前面规定的乘法运算也不是交换群.实际上,设$m=m_1m_2$, $1<m_1, m_2<m$, 那么$m_1, m_2\in\mathbf{Z}_m\backslash\{0\}$, 而

$$m_1\odot m_2=(m_1m_2)_m=(m)_m=0.$$

因此, 这时$\mathbf{Z}_m\backslash\{0\}$对于前面规定的乘法运算甚至都不自封.

但是如果我们引进集合

$$\mathbf{Z}_m^* = \{a \mid a \in \mathbf{Z}_m \text{ 而且 } (a, m) = 1\},$$

那么我们可以证明 $\mathbf{Z}_m^*$ 对于模 m 乘法运算

$$a \odot b = (ab)_m$$

来说是一个交换群.

首先来证明 $\mathbf{Z}_m^*$ 对于模 m 乘法运算是自封的. 设 $a, b \in \mathbf{Z}_m^*$, 即 $0 < a, b < m$ 而 $(a, m) = (b, m) = 1$. 显然从 $(a, m) = (b, m) = 1$ 可推出 $(ab, m) = 1$. 设用 m 去除 ab 所得的商是 q, 余数是 $(ab)_m$, 即

$$ab = qm + (ab)_m, \quad 0 \leqslant (ab)_m < m.$$

由上式可知 $\qquad (ab, m) = ((ab)_m, m).$

今 $(ab, m) = 1$, 所以 $((ab)_m, m) = 1$. 这证明了

$$a \odot b = (ab)_m \in \mathbf{Z}_m^*.$$

再证明 $\mathbf{Z}_m^*$ 中的模 m 乘法运算满足运算规则 1), 2), 3), 4). $\mathbf{Z}_m^*$ 中的乘法运算满足交换律和结合律可仿照§1例4关于 $\mathbf{Z}_p$ 是域的有关证明证之,我们就不重复了. 又显然 $\mathbf{1}$ 是 $\mathbf{Z}_m^*$ 的单位元素, 故 3) 也成立. 现在来证明 4) 也成立.

设 $a \in \mathbf{Z}_m^*$. 因 $(a, m) = 1$, 故有整数 c 和 d 存在使

$$1 = ca + dm.$$

由上式可知, $(c, m) = 1$. 因此也有 $((c)_m, m) = 1$, 即 $(c)_m \in \mathbf{Z}_m^*$. 又有

$$\begin{aligned} 1 = ca + dm &= (ca + dm)_m = (ca)_m \\ &= ((c)_m \cdot a)_m = (c)_m \odot a. \end{aligned}$$

因此 $(c)_m = a^{-1}$. 所以 4) 也成立.

这证明了 $\mathbf{Z}_m^*$ 是交换群.

例 2 设 F 是任意域, $f(x)$ 是 $F[x]$ 中任一次数 >1 的多项式. 令

$$F[x]^*_{f(x)}=\{a(x)\mid a(x)\in F[x],\ \partial^0 a(x)<\partial^0 f(x)\text{而}$$
$$(a(x),f(x))=1\}.$$

在 $F[x]^*_{f(x)}$ 中引进乘法运算，对任意 $a(x)$，$b(x)\in F[x]^*_{f(x)}$，令

$$a(x)\odot b(x)=(a(x)b(x))_{f(x)},$$

那么完全平行于例 1 可证 $F[x]^*_{f(x)}$ 是个交换群，我们就不重复了.

我们再从交换群的公理出发，推导交换群的运算所满足的另一些运算规则，我们把它们概括在下面这个定理里.

定理 3 设 G 是个交换群，它的运算符号记作"$\cdot$"，那么 G 中以下运算规则也成立.

i)（消去律）. 设 $a, b, c\in G$ 而 $a\cdot b=a\cdot c$，那么一定有 $b=c$.

ii) 设 a, b 是 G 中任意两个元素，那么 $(a\cdot b)^{-1}=a^{-1}\cdot b^{-1}$.

iii) 设 a 是 G 中任意元素，那么

$$(a^{-1})^{-1}=a.$$

证. 设 $a\cdot b=a\cdot c$. 根据 4)，a 的逆元素 $a^{-1}\in G$. 于是

$$\begin{aligned}b&=e\cdot b=(a\cdot a^{-1})\cdot b=(a^{-1}\cdot a)\cdot b\\&=a^{-1}\cdot(a\cdot b)=a^{-1}\cdot(a\cdot c)=(a^{-1}\cdot a)\cdot c\\&=(a\cdot a^{-1})\cdot c=e\cdot c=c.\end{aligned}$$

因此 i) 成立.

其次我们有

$$(a\cdot b)\cdot(a\cdot b)^{-1}=e.$$

另一方面，又有

$$\begin{aligned}(a\cdot b)\cdot(a^{-1}\cdot b^{-1})&=(a\cdot b)\cdot(b^{-1}\cdot a^{-1})\\&=a\cdot(b\cdot(b^{-1}\cdot a^{-1}))=a\cdot((b\cdot b^{-1})\cdot a^{-1})\\&=a\cdot(e\cdot a^{-1})=a\cdot a^{-1}=e.\end{aligned}$$

由逆元素的唯一性（即定理 1 中的 ii)），可知

$$(a\cdot b)^{-1}=a^{-1}\cdot b^{-1}.$$

因此 ii) 成立.

最后我们有

$$a^{-1}\cdot a=a\cdot a^{-1}=e,$$

$$a^{-1}\cdot(a^{-1})^{-1}=e.$$

仍根据逆元素的唯一性可知

$$(a^{-1})^{-1}=a.$$

因此 iii) 也成立.

设 G 是任意一群, a 是 G 中任一元素, 而 n 是个正整数. 定义

$$a^n=\underbrace{a\cdot a\cdot\cdots\cdot a}_{n\text{个}},$$

$$a^0=e,$$

$$a^{-n}=(a^{-1})^n.$$

那么可以证明下面这些运算规则成立:

i) 对任意 $a, b\in G$ 和任意整数 n, 有

$$(a\cdot b)^n=a^n\cdot b^n.$$

ii) 对任意 $a\in G$ 和任意整数 m, n, 有

$$a^{m+n}=a^m\cdot a^n,$$

$$a^{mn}=(a^m)^n.$$

由于证明都很简单,我们就不写出来了.

定义 3 设 G 是任意交换群. 如果 G 含无限多个元素, G 就叫无限交换群. 如果 G 仅含有限个元素, G 就叫有限交换群; 而 G 中元素的个数就叫做 G 的阶, 记作 $|G|$.

例如, 有理数域 $\mathbf{Q}$ 的乘法群 $\mathbf{Q}^*$ 是个无限交换群; 有限域 $\mathbf{Z}_p$ 的乘法群 $\mathbf{Z}_p^*$ 是个有限交换群, 而它的阶是 $p-1$.

例 1 中的群 $\mathbf{Z}_m^*$ 也是有限交换群, 我们把它的阶记作 $\varphi(m)$. $\varphi(m)$ 称为欧拉 (Euler) φ 函数, 它等于 $<m$ 的正整数中与 m 互素的个数. 如果 m 的素因数分解式是

$$m=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r},$$

其中 $p_1, p_2, \cdots, p_r$ 是两两不相等的素数，而 $e_1, e_2, \cdots, e_r$ 都是 $\geqslant 1$ 的整数，那么

$$\varphi(m)=\prod_{i=1}^{r} p_i^{e_i-1}(p_i-1).$$

这个公式的证明将在 §8 中给出.

定义 4 设 G 是交换群，而 a 是 G 中任意一个元素. 如果对于任意正整数 n，都有 $a^n\neq e$，a 就叫做一个无限阶元素. 如果有正整数 n 使 $a^n=e$，a 就叫做一个有限阶元素，而具有性质 $a^n=e$ 的最小正整数 n 就叫做 a 的阶.

根据 §3 定理 2 可知，当 F 是特征 0 的域时，F 的加法群中任一 $\neq 0$ 的元素都是无限阶的；而当 F 是特征 p 的域时，F 的加法群中任一 $\neq 0$ 的元素都是 p 阶元素.

定理 4 设 G 是个有限交换群，那么 G 中任一元素都是有限阶的. 设 a 是 G 的一个 n 阶元素，那么下面这 n 个元素

$$a^0=e,\ a^1=a,\ a^2,\ a^3,\ \cdots,\ a^{n-1} \tag{2}$$

是 G 中 n 个两两不同的元素，a 的任意次幂(正、负或 0)皆在其中，而且 $a^m=e$，当且仅当 $n|m$. 更进一步，令

$$[a]=\{a^0, a^1, a^2, \cdots, a^{n-1}\},$$

那么 $[a]$ 对于 G 中运算来说是一个 n 阶交换群.

证. 设 $a\in G$. 因 G 的元素个数有限，下面这一系列元素

$$a^0=e,\ a^1=a,\ a^2,\ a^3,\ \cdots$$

不能两两不同. 设 $a^j=a^k$，$0\leqslant j<k$，那么

$$a^{k-j}=a^k\cdot a^{-j}=a^j\cdot(a^{-1})^j=(a\cdot a^{-1})^j=e^j=e,$$

而 $k-j>0$. 因此 a 是有限阶的.

现在设 a 是 G 的一个 n 阶元素. 假定 $a^{m_1}=a^{m_2}$，$0\leqslant m_1<m_2<n$，那么 $a^{m_2-m_1}=e$. 因 a 的阶是 n，而 $0\leqslant m_2-m_1<n$，所以一定有 $m_2-m_1=0$，即 $m_1=m_2$. 这证明了(2)中 n 个元素

两两不同.

设m是任意整数. 再设用n去除m所得的商是q而余数是$(m)_n$, 即

$$m=qn+(m)_n,\ 0\leqslant(m)_n<n.$$

那么
$$a^m=a^{qn+(m)_n}=a^{qn}\cdot a^{(m)_n}=(a^n)^q\cdot a^{(m)_n}$$
$$=e^q\cdot a^{(m)_n}=e\cdot a^{(m)_n}=a^{(m)_n}.$$

因$a^{(m)_n}$在(2)中, 所以a^m也在(2)中. 更进一步, 由上式显然有$a^m=e$, 当且仅当$a^{(m)_n}=e$. 但$0\leqslant(m)_n<n$, 因此$a^m=e$, 当且仅当$(m)_n=0$, 即$n|m$.

最后来证明$[a]$对于G中运算来说是一个交换群. 因交换律和结合律对于G中元素来说都成立, 所以对于$[a]$中元素来说也成立. 显然$a^0=e$是$[a]$的单位元素. 又对于任意$a^k\in[a]$, $0\leqslant k<n$, 我们有$a^{n-k}\in[a]$, 而且有

$$a^k\cdot a^{n-k}=a^n=e.$$

因此$[a]$中任一元素的逆元素都在其中. 这证明了$[a]$是个n阶交换群.

在这里我们附带地提一下, 同子域的概念一样, 也可以定义子群的概念. 设G是一个群, 而G_0是G的一个非空子集. 如果G_0对于G中的运算来说是一个群, 这就是说, 对于G_0中任意两个元素按G中运算进行运算所得结果仍是G_0中的元素而且G中运算对于G_0来说也满足定义1中的运算规则2), 3), 4), 我们就说G_0是G的子群. 这样一来, 定理4的最后一个断言实际上是说, 如果a是有限交换群中的一个n阶元素, 那么$[a]=\{a^0, a^1, a^2, \cdots, a^{n-1}\}$就是$G$的一个$n$阶子群.

同域的同构这个概念一样, 我们也可以定义群的同构. 设G和G'是两个群. 如果可以在G和G'的元素之间建立一个一一对应

$$\sigma: a\to\sigma(a)\quad(a\in G,\ \sigma(a)\in G'),$$

而且这个一一对应保持群的运算，这就是说，G 中任意两个元素 a 与 b 的积 $a\cdot b$ 对应到 a 的象 $\sigma(a)$ 与 b 的象 $\sigma(b)$ 的积 $\sigma(a)\cdot\sigma(b)$，也就是说，这个一一对应 σ 适合条件：

$$\sigma(ab)=\sigma(a)\sigma(b),\quad 对任意\ a,\ b\in G,$$

我们就说 G 和 G' 同构，而 σ 是从 G 到 G' 的一个同构映射，或同构对应，或简称同构. 同 §2 定理 4 一样，可以证明，如果 σ 是从群 G 到群 G' 的一个同构映射，那么 σ 一定将 G 的单位元素 e 映到 G' 的单位元素，σ 也一定将 G 中任一元素 a 的逆元素 a^{-1} 映到 a 的象 $\sigma(a)$ 的逆 $\sigma(a)^{-1}$.

定义 5 设 G 是个 n 阶交换群. 如果 G 中有一个 n 阶元素 a 存在，那么

$$G=[a]=\{a^0=e,\ a^1=a,\ a^2,\ \cdots,\ a^{n-1}\},$$

就叫做(n 阶)循环群，而 a 叫做 G 的一个生成元.

在 §2 中我们曾经指出，$\mathbf{F}_{2^2}^*$ 中有两个 3 阶元素，$\mathbf{F}_{3^2}^*$ 中有 4 个 8 阶元素. 因此 $\mathbf{F}_{2^2}^*$ 和 $\mathbf{F}_{3^2}^*$ 都是循环群. 下面我们主要要证明，任一有限域的乘法群都是循环群，而且还要算出它的生成元的个数. 但需要先做一些准备.

引理 1 设 G 是个有限交换群，a 是 G 的一个 n 阶元素，k 是任意整数，那么 a^k 是个 $n/(k,\ n)$ 阶元素. 特别 a^k 是 n 阶元素，当且仅当 $(k,\ n)=1$.

证. 显然有

$$(a^k)^{\frac{n}{(k,n)}}=a^{\frac{kn}{(k,n)}}=(a^n)^{\frac{k}{(k,n)}}=e^{\frac{k}{(k,n)}}=e.$$

设 m 是 a^k 的阶，那么由定理 4 可知

$$m\,\Big|\,\frac{n}{(k,\ n)}. \tag{3}$$

另一方面又有 $\qquad a^{km}=(a^k)^m=e.$

因为 a 是个 n 阶元，所以仍由定理 4 可知 $n\,|\,km$. 写

$$n=\frac{n}{(k, n)}\cdot(k, n), \quad k=\frac{k}{(k, n)}\cdot(k, n).$$

则从 $n|km$ 推出

$$\frac{n}{(k, n)}\Bigg|\frac{k}{(k, n)}\cdot m.$$

但

$$\left(\frac{n}{(k, n)}, \frac{k}{(k, n)}\right)=1,$$

所以

$$\frac{n}{(k, n)}\Bigg|m. \tag{4}$$

于是由(3)和(4)推出

$$m=\frac{n}{(k, n)}.$$

系理 设 G 是个 n 阶循环群，a 是它的一个生成元，k 是任意整数，那么 a^k 也是 G 的生成元，当且仅当 $(k, n)=1$.

证. 根据引理 1, a^k 的阶是 $n/(k, n)$. 但 a^k 是 G 的生成元，当且仅当 a^k 的阶是 n. 因此 a^k 是 G 的生成元，当且仅当 $(k, n)=1$.

引理 2 设 G 是个有限交换群，a 是 G 的一个 m 阶元素，b 是 G 的一个 n 阶元素. 并假定 $(m, n)=1$, 那么 ab 就是一个 mn 阶元素.

证. 显然有

$$(ab)^{mn}=(a^m)^n(b^n)^m=e^n\cdot e^m=e\cdot e=e.$$

设 ab 的阶是 l, 则根据定理 4, 有

$$l|mn.$$

另一方面，由

$$(ab)^l=e$$

推出

$$a^l=b^{-l}.$$

根据引理 1, a^l 的阶是 m 的因数，b^{-l} 的阶是 n 的因数. 因此 $a^l=b^{-l}$ 的阶是 (m, n) 的因数. 但假定 $(m, n)=1$, 所以 $a^l=b^{-l}$

是 1 阶元素，即

$$a^l=b^{-l}=e.$$

故根据定理 4，有

$$m|l,\ n|l.$$

仍因 $(m, n)=1$，所以

$$mn|l.$$

因此一定有 $l=mn$.

引理 3 设 G 是个有限交换群. 假定 G 的元素的阶中 n 是最大的，那么 G 中任一元素的阶一定是 n 的因数.

证. 设 a 是 G 中一个 n 阶元素，而 $n \geqslant G$ 中任一元素的阶. 设 b 是 G 中任一元素，并假定 b 的阶是 m. 如果 $m \nmid n$，那么一定有一个素数 p，它在 m 中出现的幂次大于它在 n 中出现的幂次，即

$$n=p^{e_1}n_1,\ m=p^{e_2}m_1,$$
$$(p,\ n_1)=(p,\ m_1)=1,$$
$$e_2>e_1.$$

那么根据引理 1，$a^{p^{e_1}}$ 就是 G 中一个 n_1 阶元素，而 b^{m_1} 就是 G 中一个 p^{e_2} 阶元素. 但

$$(n_1,\ p^{e_2})=1,$$

因此根据引理 2，$a^{p^{e_1}}b^{m_1}$ 就是 G 中一个 $p^{e_2}n_1$ 阶元素. 但

$$p^{e_2}n_1>p^{e_1}n_1=n,$$

这与 n 的最大性相矛盾. 因此一定有 $m|n$.

现在我们来证明

定理 5 任一有限域的乘法群都是循环群.

证. 设 F 是个有限域，它的元素个数是 q，那么 F^* 是个 $q-1$ 阶的有限交换群. 在 F^* 中一定有一个最大阶的元素. 设 a 是 F^* 中的一个最大阶元素，并设 a 的阶是 n. 那么根据定理 4，

$$e,\ a,\ a^2,\ \cdots,\ a^{n-1}$$

就是 F^* 中 n 个两两相异的元素. 但 F^* 一共有 $q-1$ 个元素，因此一定有

$$n \leqslant q-1.$$

另一方面，根据引理 3, F^* 中任一元素的阶都是 n 的因数. 那么根据定理 4, F^* 中任一元素均适合多项式

$$x^n - e.$$

但 F^* 一共有 $q-1$ 个元素. 因此根据 §2 定理 5 的系理 2, 一定有

$$q-1 \leqslant n.$$

所以
$$n = q-1.$$

这证明了 F^* 是由 a 生成的循环群.

定义 6 有限域的乘法群的生成元叫做这个有限域的*本原元*.

系理 设 F 是元素个数为 q 的有限域, 那么 F 总共有 $\varphi(q-1)$ 个本原元.

证. 设 a 是 F^* 的一个生成元, 即 F 的一个本原元. 则根据定理 4,

$$a^0 = e,\ a^1 = a,\ a^2,\ \cdots,\ a^{q-2}$$

就是 F^* 的全部 $q-1$ 个元素. 再根据引理 1 的系理, $a^k(0 \leqslant k < q-1)$ 是 F^* 的生成元, 当且仅当 $(k,\ q-1)=1$. 因此 F^* 的生成元(即 F 的本原元)的总数是 $\varphi(q-1)$.

§5 有限域的结构

在这一节里, 我们将证明有限域的三条结构定理, 它们是

定理 1 设 F 是有限域并设 F 的特征是 p, 那么 F 的元素个数一定是 p 的一个幂.

定理 2 设 p 是任一素数而 n 是任一正整数，那么总存在着一个恰含 p^n 个元素的有限域.

定理 3 任意两个元素个数相同的有限域一定同构.

我们先来证明定理 1 的一个推广，它包有定理 1 作为特例.

定理 4 设 F 是个有限域，它包有一个 q 个元素的有限域 F_q 作为子域，那么 F 的元素个数一定是 q 的一个幂.

证. 将 F_q 改记成 F_1. 如果 $F=F_1$，那么 F 就是恰含 q 个元素的有限域. 因此这时定理 4 成立. 如果 $F\neq F_1$，那么 F 就含有一个元素 e_2，而 $e_2\notin F_1$. 令

$$F_2=\{a_1+a_2e_2 \mid a_1,\ a_2\in F_1\}.$$

我们证明：如果

$$a_1+a_2e_2=b_1+b_2e_2,\quad a_1,\ a_2,\ b_1,\ b_2\in F_1,$$

那么就一定有 $a_1=b_1$，$a_2=b_2$. 实际上，从上式推出

$$(a_2-b_2)e_2=b_1-a_1.$$

如果 $a_2\neq b_2$，那么

$$e_2=(a_2-b_2)^{-1}(b_1-a_1)\in F_1.$$

这是一个矛盾. 因此一定有 $a_2=b_2$. 于是也有 $a_1=b_1$. 因此可以推出 F_2 恰含 q^2 个两两不同的元素.

如果 $F=F_2$，那么 F 就是恰含 q^2 个元素的有限域. 因此这时定理 4 成立. 如果 $F\neq F_2$，那么 F 就含有一个元素 e_3，而 $e_3\notin F_2$. 令

$$F_3=\{a_1+a_2e_2+a_3e_3 \mid a_1,\ a_2,\ a_3\in F_1\}.$$

假定有 $\quad a_1+a_2e_2+a_3e_3=b_1+b_2e_2+b_3e_3,\ a_i,\ b_i\in F_1.$

则有 $\quad (a_3-b_3)e_3=((b_1-a_1)+(b_2-a_2)e_2).$

如果 $a_3\neq b_3$，那么

$$e_3=(a_3-b_3)^{-1}(b_1-a_1)+(a_3-b_3)^{-1}(b_2-a_2)e_2\in F_2.$$

这是一个矛盾. 因此一定有 $a_3=b_3$. 于是有

$$a_1+a_2e_2=b_1+b_2e_2,$$

再根据上一段的证明可知 $a_1=b_1$, $a_2=b_2$. 于是可以推出 F_3 恰含 q^3 个两两不同的元素.

如果 $F=F_3$, 那么 F 就是恰含 q^3 个元素的有限域. 因此这时定理 4 成立. 如果 $F\neq F_3$, 那么 F 就含有一个元素 e_4, $e_4\notin F_3$. 令

$$F_4=\{a_1+a_2e_2+a_3e_3+a_4e_4 \mid a_1,\ a_2,\ a_3,\ a_4\in F_1\}.$$

仿上可证 F_4 恰含 q^4 个两两不同的元素.

如此继续下去. 如果 F 的元素个数是 N, 而 $q^n\leqslant N<q^{n+1}$, 那么我们就得到 F 的一串子集

$$F_1,\ F_2,\ F_3,\ \cdots,\ F_n,$$

其中 $$F_i=\{a_1+a_2e_2+\cdots+a_ie_i \mid a_1,\ a_2,\ \cdots,\ a_i\in F_1\},$$

而 $$e_2\notin F_1,\ e_3\notin F_2,\ \cdots,\ e_n\notin F_{n-1},$$

同时 $F_i(1\leqslant i\leqslant n)$ 恰含 q^i 个两两不同的元素. 如果 $F\neq F_n$, 那么 F 就含有一个元素 e_{n+1}, $e_{n+1}\notin F_n$. 令

$$F_{n+1}=\{a_1+a_2e_2+\cdots+a_ne_n+a_{n+1}e_{n+1} \mid a_1,\ a_2,\ \cdots,\ a_n,\ a_{n+1}\in F_1\}.$$

仿上可证 F_{n+1} 恰含 q^{n+1} 个两两不同的元素. 但 F_{n+1} 是 F 的子集, 而 F 的元素个数 $N<q^{n+1}$. 所以这是不可能的. 因此一定有 $F=F_n$. 于是 F 是恰含 q^n 个元素的有限域. 这证明了定理 4.

从定理 4 立刻可以导出定理 1. 设 F 是有限域, 并设 F 的特征是 p, 那么 p 一定是个素数, 而 F 的素域 Π 就是恰含 p 个元素的有限域. 在定理 4 中取 $F_q=\Pi$, 就得出定理 1.

为了证明定理 2, 只要证明: 对于任一素数 p 和任一正整数 n, $\mathbf{Z}_p[x]$ 中总有一个 n 次不可约多项式即可. 因为如果

$f(x)$ 是 $\mathbf{Z}_p[x]$ 中的一个 n 次不可约多项式，那么在 §2 中构造的域 $\mathbf{Z}_p[x]_{f(x)}$ 就是一个 p^n 个元素的有限域. 下面我们将求出任一有限域上 n 次不可约多项式的个数的一个显明公式，然后再利用这个公式推出这个个数一定 $\geqslant 1$. 特别，我们就证明了 $\mathbf{Z}_p[x]$ 中总有 n 次不可约多项式存在.

为了求出任一有限域上 n 次不可约多项式的个数的一个公式，需要先做一些准备.

引理 1 设 F 是个有限域，而 F_q 是 F 的一个含 q 个元素的子域，那么 F_q 中的元素 α 都适合条件 $\alpha^q=\alpha$. 更进一步，如果 F 中有一个元素 β 适合条件 $\beta^q=\beta$，那么 $\beta\in F_q$.

证. 根据 §4 定理 5，我们知道 F_q^* 是 $q-1$ 阶循环群. 设 ξ 是它的一个生成元，那么

$$\xi^0=e,\ \xi^1=\xi,\ \xi^2,\ \cdots,\ \xi^{q-2}$$

就是 F_q^* 的全部 $q-1$ 个元素. 显然有

$$(\xi^i)^{q-1}=(\xi^{q-1})^i=e^i=e,\ 0\leqslant i\leqslant q-2.$$

将上式两端同乘以 ξ^i，就有

$$(\xi^i)^q=\xi^i,\ 0\leqslant i\leqslant q-2.$$

这就是说，F_q 中任一元素 α (包括 0) 都适合条件 $\alpha^q=\alpha$. 这样一来，多项式

$$x^q-x$$

就以 F_q 中的 q 个元素为它的全部根. 将 x^q-x 看作 F 上的多项式，它在 F 中顶多有 q 个根. 因此如果有 $\beta(\in F)$ 是这个多项式的根，即 $\beta^q-\beta=0$，那么一定有 $\beta\in F_q$.

引理 2 设 F_q 是 q 个元素的一个有限域，而 $f(x)$ 是 $F_q[x]$ 中的一个 n 次不可约多项式，那么一定有

$$f(x)\mid x^{q^n}-x.$$

证. 令

$$F_q[x]_{f(x)}=\{a_0+a_1x+a_2x^2+\cdots$$
$$+a_{n-1}x^{n-1}\,|\,a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1}\in F_q\}.$$

在§2中已经在 $F_q[x]_{f(x)}$ 中规定了加法和乘法运算，即对任意 $a(x)$，$b(x)\in F_q[x]_{f(x)}$，规定

$$a(x)\oplus b(x)=a(x)+b(x),$$
$$a(x)\odot b(x)=(a(x)\cdot b(x))_{f(x)}.$$

我们也证明了 $F_q[x]_{f(x)}$ 按如上规定的加法和乘法运算是一个域，而且是一个含 q^n 个元素的域．根据引理1，$F_q[x]_{f(x)}$ 中的元素 α 都适合条件 $\alpha^{q^n}=\alpha$，即 $\alpha^{q^n}-\alpha=0$．特别，$x\in F_q[x]_{f(x)}$．因此在 $F_q[x]_{f(x)}$ 中 $x^{q^n}-x=0$，而这实际上是

$$\underbrace{x\odot x\odot\cdots\odot x}_{q^n\text{个}}-x=0,$$

即
$$(x^{q^n})_{f(x)}-x=0.$$

但根据§2定理1的系理有

$$(x^{q^n}-x)_{f(x)}=(x^{q^n})_{f(x)}-x,$$

因此
$$(x^{q^n}-x)_{f(x)}=0,$$

这就是说
$$f(x)\,|\,x^{q^n}-x.$$

引理3 设 F_q 是 q 个元素的一个有限域，而 $f(x)$ 是 $F_q[x]$ 中的一个 m 次不可约多项式，如果 $m>n$，那么一定有

$$f(x)\nmid x^{q^n}-x.$$

证．用反证法．设 $f(x)\,|\,x^{q^n}-x$．这就是说，$(x^{q^n}-x)_{f(x)}=0$．因此

$$(x^{q^n})_{f(x)}=x.$$

因 $\partial^0 f(x)=m$，所以 $F_q[x]_{f(x)}$ 是 q^m 个元素的有限域． 又因 F_q 是 $F_q[x]_{f(x)}$ 的子域，所以 q 一定是 $F_q[x]_{f(x)}$ 的特征（也是 F_q 的特征）的一个幂．那么对于 $F_q[x]_{f(x)}$ 中任意一个元素

$$g(x)=\sum_{i=0}^{m-1}a_ix^i,\quad a_i\in F_q,$$

都有
$$g(x)\underbrace{\odot g(x)\odot\cdots\odot}_{q^n\text{个}} g(x)-g(x)$$
$$=(g(x)^{q^n})_{f(x)}-g(x)$$
$$=\left(\sum_{i=0}^{m-1} a_i^{q^n} x^{iq^n}\right)_{f(x)}-\sum_{i=0}^{m-1} a_i x^i$$
$$=\sum_{i=0}^{m-1} a_i(((x^{q^n})_{f(x)})^i)_{f(x)}-\sum_{i=0}^{m-1} a_i x^i$$
$$=\sum_{i=0}^{m-1} a_i x^i-\sum_{i=0}^{m-1} a_i x^i=0.$$
这就是说，$F_q[x]_{f(x)}$ 中 q^m 个元素都适合多项式
$$X^{q^n}-X.$$
但 $m>n$，因此根据 § 2 定理 5 的系理 2，这是不可能的．这就证明了引理 3.

引理 4 设 m, n 是正整数，而 $d=(m, n)$，那么
$$(x^m-e,\ x^n-e)=x^d-e.$$

证．对 $\max(m, n)$ 用归纳法．当 $m=n$ 时，本引理显然成立．设 $m>n$，那么
$$(x^m-e,\ x^n-e)=(x^m-e-x^{m-n}(x^n-e),\ x^n-e)$$
$$=(x^{m-n}-e,\ x^n-e).$$
但 $\max(m-n, n)<m=\max(m, n)$，而 $(m-n, n)=(m, n)=d$，所以根据归纳法假设有
$$(x^{m-n}-e,\ x^n-e)=x^d-e.$$
因此
$$(x^m-e,\ x^n-e)=x^d-e.$$

引理 5 设 m, n 是正整数，而 $d=(m, n)$，那么
$$(x^{q^m}-x,\ x^{q^n}-x)=x^{q^d}-x.$$

证．仿照引理 4 的证明，可证
$$(q^m-1,\ q^n-1)=q^d-1,$$
那么根据引理 4，有
$$(x^{q^m-1}-e,\ x^{q^n-1}-e)=x^{q^d-1}-e,$$

因此 $$(x^{q^m}-x,\ x^{q^n}-x)=x^{q^d}-x.$$

引理6 设 F_q 是一个 q 个元素的有限域，而 $f(x)$ 是 $F_q[x]$ 中的一个 d 次不可约多项式，那么 $f(x)\mid x^{q^n}-x$，当且仅当 $d\mid n$.

证. 根据引理2，

$$f(x)\mid x^{q^d}-x.$$

如果 $d\mid n$，则 $(d,\ n)=d$，根据引理5，

$$(x^{q^d}-x,\ x^{q^n}-x)=(x^{q^d}-x),$$

于是 $$f(x)\mid(x^{q^d}-x,\ x^{q^n}-x),$$

因此 $$f(x)\mid x^{q^n}-x.$$

反之，设 $$f(x)\mid x^{q^n}-x,$$

那么 $$f(x)\mid(x^{q^n}-x,\ x^{q^d}-x),$$

令 $d'=(n,\ d)$. 根据引理5，就有

$$f(x)\mid x^{q^{d'-1}}-x.$$

再根据引理3，$d'\geqslant d$. 但 $d'=(n,\ d)\leqslant d$. 因此 $d'=d$. 于是 $d\mid n$.

引理7 设 F_q 是一个 q 个元素的有限域. 那么对于任意正整数 n，$x^{q^n}-x$ 都没有重因式.

证. 令 $$f(x)=x^{q^n-1}-e,$$

那么 $$f'(x)=(q^n-1)x^{q^n-2}.$$

设 F_q 的特征为 p. 根据定理1，q 是 p 的一个幂. 设 $q=p^m$，那么

$$(q^n-1,\ p)=(p^{mn}-1,\ p)=1.$$

因此 $f'(x)\neq 0$. 但 $f'(x)$ 只有 x 及 $cx\,(c\in F_q)$ 为其因式，而 $x\nmid f(x)$，因此

$$(f(x),\ f'(x))=e.$$

那么根据§2定理4，$x^{q^n-1}-e$ 没有重因式. 又显然 x 不是 $x^{q^n-1}-e$ 的因式. 因此 $x^{q^n}-x$ 也没有重因式.

有了上面这些准备，我们先来证明

定理5 设 F_q 是一个 q 个元素的有限域，n 是一个正整

数，而 $p_1, p_2, \cdots, p_m$ 是 n 的所有两两不同的素因数．用 $\Phi_{q,n}(x)$ 表示 $F_q[x]$ 中所有首项系数是 e 的 n 次不可约多项式的乘积，那么

$$\Phi_{q,n}(x)=(x^{q^n}-x)\cdot\prod_{i=1}^{m}(x^{q^{n/p_i}}-x)^{-1}$$

$$\cdot\prod_{1\leqslant i<j\leqslant m}(x^{q^{n/p_ip_j}}-x)\cdot\prod_{1\leqslant i<j<k\leqslant m}(x^{q^{n/p_ip_jp_k}}-x)^{-1}$$

$$\cdots\cdots(x^{q^{n/p_1p_2\cdots p_m}}-x). \tag{1}$$

再用 $|\Phi_{q,n}|$ 表示 $F_q[x]$ 中首项系数是 e 的 n 次不可约多项式的个数，那么

$$|\Phi_{q,n}|=\frac{1}{n}\Big(q^n-\sum_{i=1}^{m}q^{n/p_i}+\sum_{1\leqslant i<j\leqslant m}q^{n/p_ip_j}$$

$$-\sum_{1\leqslant i<j<k\leqslant m}q^{n/p_ip_jp_k}+\cdots+(-1)^m q^{n/p_1p_2\cdots p_m}\Big). \tag{2}$$

证．在引理 7 里已经证明 $x^{q^n}-x$ 没有重因式，因此根据 §2 定理 3，$x^{q^n}-x$ 可以分解成 $F_q[x]$ 中一些两两不同的首项系数是 e 的不可约多项式的乘积．再根据引理 6 可知，$x^{q^n}-x$ 是 $F_q[x]$ 中所有次数是 n 的因数的首项系数是 e 的不可约多项式的乘积．为了从 $x^{q^n}-x$ 得到 $\Phi_{q,n}(x)$，需要从 $x^{q^n}-x$ 中除去所有次数是 n/p_1，或 n/p_2，$\cdots$，或 n/p_m 的因数的首项系数是 e 的不可约多项式．仍根据引理 6，次数是 n/p_i 的因数的首项系数是 e 的不可约多项式的乘积正好是 $x^{q^{n/p_i}}-x\,(1\leqslant i\leqslant m)$．但从 $x^{q^n}-x$ 除去 $\prod_{i=1}^{m}(x^{q^{n/p_i}}-x)$ 之后，在

$$(x^{q^n}-x)\cdot\prod_{i=1}^{m}(x^{q^{n/p_i}}-x)^{-1}$$

中，次数是 $\dfrac{n}{p_ip_j}$ $(1\leqslant i<j\leqslant m)$ 的因数的首项系数是 e 的不可约多项式却被除去了两次，故又需添上，但在添上 $\prod_{1\leqslant i<j\leqslant m}(x^{q^{n/p_ip_j}}-x)$ 之后，在

$$(x^{q^n}-x)\cdot\prod_{i=1}^{m}(x^{q^{n/p_i}}-x)^{-1}\cdot\prod_{1\leqslant i<j\leqslant m}(x^{q^{n/p_ip_j}}-x)$$

中，以 $\dfrac{n}{p_ip_jp_l}$ $(1\leqslant i<j<k\leqslant m)$的因数为次数的首项系数是 e 的不可约多项式先被除去了 3 次，后又被添上了 $\binom{3}{2}=3$ 次，故仍需除去. 如此继续下去，即得(1)式.

当然也可以直接验证(1)式成立. 首先，$F_q[x]$ 中次数 n 的首项系数是 e 的任一不可约多项式显然在(1)式双方各出现一次. 其次，设 $\varphi(x)$ 是 $F_q[x]$ 中任一次数 d 的首项系数是 e 的不可约多项式，$d|n$ 而 $d\neq n$. 重排 $p_1, p_2, \cdots, p_m$ 之后，可设

$$n=p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m},$$
$$d=p_1^{f_1}p_2^{f_2}\cdots p_r^{f_r}p_{r+1}^{e_{r+1}}\cdots p_m^{e_m},$$
$$f_1<e_1,\ f_2<e_2,\ \cdots,\ f_r<e_r,$$

那么在

$$\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_s}}\ (0\leqslant s\leqslant m,\ 1\leqslant i_1<i_2<\cdots<i_s\leqslant m)$$

这些数中，只有

$$n,\ \frac{n}{p_i}\ (1\leqslant i\leqslant r),$$

$$\frac{n}{p_ip_j}\ (1\leqslant i<j\leqslant r),\ \cdots,\ \frac{n}{p_1p_2\cdots p_r}$$

以 d 为因数，因此在

$$x^{q^{n/p_{i_1}p_{i_2}\cdots p_{i_s}}}-x\ (0\leqslant s\leqslant m,$$
$$1\leqslant i_1<i_2<\cdots<i_s\leqslant m)$$

这些多项式中，只有

$$x^{q^n}-x,\ x^{q^{n/p_i}}-x\ (1\leqslant i\leqslant r),$$

$$x^{q^{n/p_ip_j}}-x\ (1\leqslant i<j\leqslant r),\ \cdots,\ x^{q^{n/p_1p_2\cdots p_r}}-x$$

以 $\varphi(x)$ 为因式. 因此 $\varphi(x)$ 在(1)式右方出现的次数是

$$1-\binom{r}{1}+\binom{r}{2}-\cdots+(-1)^r=(1-1)^r=0.$$

最后，设 $\psi(x)$ 是 $F_q[x]$ 中次数 l 的首项系数是 e 的任一不可约多项式，而 $l\nmid n$. 那么显然 $\psi(x)$ 在(1)式双方均不出现. 这样又给出(1)式的另一证明.

比较(1)式双方的次数就得出

$$n|\Phi_{q,n}|=q^n-\sum_{i=1}^{m}q^{n/p_i}+\sum_{1\leqslant i<j\leqslant m}q^{n/p_ip_j}$$
$$-\sum_{1\leqslant i<j<k\leqslant m}q^{n/p_ip_jp_k}+\cdots+(-1)^m q^{n/p_1p_2\cdots p_m}. \quad (3)$$

再将上式双方除以 n 就得出(2)式.

这样定理 5 就完全证明了.

系理 $|\Phi_{q,n}|>0$.

证. 显然 $|\Phi_{q,n}|\geqslant 0$. 因此要证明这个系理，只要证明 $|\Phi_{q,n}|\neq 0$ 即可. 仍令

$$n=p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m},$$

其中 $p_1, p_2, \cdots, p_m$ 是两两不同的素数. 那么(3)式右方除最后一项之外，都是

$$q^{n/p_1p_2\cdots p_m+1}$$

的因数. 因此 $n|\Phi_{q,n}|$ 不能被 $q^{n/p_1p_2\cdots p_m+1}$ 所整除，所以 $n|\Phi_{q,n}|\neq 0$. 于是 $|\Phi_{q,n}|\neq 0$. 因此本系理成立.

特别，当 p 是任一素数，n 是任一正整数时，我们有 $|\Phi_{p,n}|>0$. 即 p 个元素的有限域 $\mathbf{Z}_p$ 上总有 n 次不可约多项式存在. 因此总有 p^n 个元素的有限域存在. 这证明了定理 2.

为了证明定理 3，先引进下面这个定义.

定义 1 设 F 是个有限域，F_q 是它的一个恰含 q 个元素的子域. 设 α 是 F 中任一元素. α 在 F_q 上的极小多项式是指 α 所适合的 $F_q[x]$ 中的首项系数为 e 的次数最低的多项式.

我们先证明几条引理.

引理8 设 F 是个有限域, F_q 是它的一个恰含 q 个元素的子域,那么 F 中任一元素在 F_q 上都有唯一的一个极小多项式,而且它是 F_q 上的不可约多项式.

证. 根据定理1, F 的元素个数一定是 q 的幂; 设为 q^n, 那么根据引理4, F 中任一元素 α 均适合 F_q 上的多项式

$$x^{q^n}-x,$$

因此 α 一定适合 F_q 上的一个首项系数为 e 的次数最低的多项式. 这证明了 α 在 F_q 上一定有一个极小多项式.

假定 α 在 F_q 上有两个极小多项式 $f(x)$ 和 $g(x)$. 那么一定有 $\partial^0 f(x)=\partial^0 g(x)$. 设 $\partial^0 f(x)=m$. 可以写

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{m-1}x^{m-1}+x^m,\quad a_i\in F_q,$$

$$g(x)=b_0+b_1x+b_2x^2+\cdots+b_{m-1}x^{m-1}+x^m,\quad b_i\in F_q.$$

那么 α 适合 F_q 上的多项式 $f(x)-g(x)$, 而 $\partial^0(f(x)-g(x))<m$. 如果 $f(x)\neq g(x)$, 那么 α 就适合一个次数 $<m$ 的非零多项式. 将这个多项式乘以它的首项系数的逆元素, 就得到 α 所适合的一个首项系数为 e 的次数 $<m$ 的多项式. 这与 $f(x)$ 是 α 的极小多项式的假设相矛盾. 因此 $f(x)=g(x)$. 这证明了 α 在 F_q 上的极小多项式的唯一性.

仍设 $f(x)$ 是 α 在 F_q 上的极小多项式, 如果 $f(x)$ 在 F_q 上可约, 即

$$f(x)=g(x)h(x),\quad 而\ \partial^0 g(x),\ \partial^0 h(x)<\partial^0 f(x),$$

将 α 代入上式得

$$f(\alpha)=g(\alpha)h(\alpha).$$

但 $f(\alpha)=0$, 因此 $g(\alpha)=0$ 或 $h(\alpha)=0$. 因

$$\partial^0 g(x),\ \partial^0 h(x)<\partial^0 f(x),$$

这样 α 就适合一个次数 $<\partial^0 f(x)$ 的多项式. 这与 $f(x)$ 是 α

的极小多项式的假设相矛盾. 因此$f(x)$是F_q上的不可约多项式.

引理 9 设F是个有限域, F_q是它的一个恰含q个元素的子域, 而α是F中任一元素. 假定α在F_q上的极小多项式$f(x)$是m次的, 那么

$$F_0=\{a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{m-1}\alpha^{m-1}$$
$$|a_0,\ a_1,\ a_2,\ \cdots,\ a_{m-1}\in F_q\}$$

是F的一个子域, 而且与$F_q[x]_{f(x)}$同构. 更进一步, 如果还假定F的元素个数是q^n, 那么m一定是n的因数.

证. 因$f(x)$是α在F_q上的极小多项式, 所以

$$\sum_{i=0}^{m-1}a_i\alpha^i=\sum_{i=0}^{m-1}b_i\alpha^i,\ a_i,\ b_i\in F_q,$$

当且仅当$a_i=b_i(i=0,\ 1,\ 2,\ \cdots,\ m-1)$. 因此$F_0$是$F$的一个$q^m$个元素的子集.

我们来证明F_0是F的子域. 显然F_0对于F中的加法运算自封. 其次设

$$\sum_{i=0}^{m-1}a_i\alpha^i,\quad \sum_{i=0}^{m-1}b_i\alpha^i(a_i,\ b_i\in F_q)$$

是F_0中任意两个元素. 令

$$a(x)=\sum_{i=0}^{m-1}a_ix^i,\quad b(x)=\sum_{i=0}^{m-1}b_ix^i.$$

根据带余除法, 可设

$$a(x)b(x)=q(x)f(x)+r(x),\ \partial^0r(x)<\partial^0f(x).$$

将$x=\alpha$代入上式得

$$a(\alpha)b(\alpha)=r(\alpha).$$

显然$r(\alpha)\in F_0$. 这证明了F_0对于F中的乘法运算也自封.

还需要验证域的公理 I.3, I.4, II.3, II.4 在F_0中成立. F的零元素 0 和单位元素e都属于F_q, 因而都属于F_0, 而且

分别是 F_0 的零元素和单位元素. 因此 I.3 和 II.3 成立. 又对任意 $\sum_{i=0}^{m-1} a_i\alpha^i \in F_0$, $\sum_{i=0}^{m-1}(-a_i)\alpha^i$ 也属于 F_0 而且

$$\sum_{i=0}^{m-1} a_i\alpha^i + \sum_{i=0}^{m-1}(-a_i)\alpha^i = 0.$$

这证明了 II.4 也成立. 最后, 设 $\sum_{i=0}^{m-1} a_i\alpha^i \neq 0$. 令

$$a(x) = \sum_{i=0}^{m-1} a_i x^i.$$

因 $f(x)$ 不可约, 而 $\partial^0 a(x) < \partial^0 f(x)$, 所以 $a(x)$ 与 $f(x)$ 互素. 于是有多项式 $c(x)$, $d(x) \in F_q[x]$, 使

$$a(x)c(x) + f(x)d(x) = e,$$

将 $x=\alpha$ 代入上式得

$$a(\alpha)c(\alpha) = e.$$

根据带余除法, 可设

$$c(x) = q(x)f(x) + r(x), \quad 而\ \partial^0 r(x) < \partial^0 f(x).$$

将 $x=\alpha$ 代入上式得

$$c(\alpha) = r(\alpha)$$

因此

$$a(\alpha)r(\alpha) = e.$$

显然 $r(\alpha) \in F_0$. 这证明了 II.4 在 F_0 中成立.

因此 F_0 是 F 的子域.

容易验证 $\sum_{i=0}^{m-1} a_i\alpha^i \to \sum_{i=0}^{m-1} a_i x^i \quad (a_i \in F_q)$

是从 F_0 到 $F_q[x]_{f(x)}$ 之上的一个同构对应.

最后, 设 F 的元素个数是 q^n. 因 F_0 是 F 的子域, 根据定理 4 一定有 $q^n = (q^m)^k$ 对某一正整数 k, 因此 m 是 n 的因数. 这样引理 9 就完全证明了.

现在来证明定理 3. 设 F 和 F' 是两个 p^n 个元素的有限域, p 是一个素数. 那么它们的素域都是 p 个元素的域, 因而

是同构的. 设 Π 和 Π' 分别是 F 和 F' 的素域, 而 0 和 $0'$ 分别是它们的零元素, e 和 e' 分别是它们的单位元素, 那么

$$\Pi=\{0,\ e,\ 2e,\ \cdots,\ (p-1)e\},$$
$$\Pi'=\{0',\ e',\ 2e',\ \cdots,\ (p-1)e'\},$$

而

$$\sigma: ke\to ke' \quad (0\leqslant k\leqslant p-1)$$

就是从 Π 到 Π' 的一个同构对应.

根据 §4 定理 5, F^* 是循环群. 设 ξ 是 F^* 的一个生成元, 并设 $f(x)$ 是 ξ 在 Π 上的极小多项式, 再设 $\partial^0 f(x)=m$, 那么根据引理 9,

$$F_0=\{a_0+a_1\xi+a_2\xi^2+\cdots+a_{m-1}\xi^{m-1}$$
$$|a_0,\ a_1,\ a_2,\ \cdots,\ a_{m-1}\in\Pi\}$$

是 F 的一个含 p^m 个元素的子域, 而且与 $\Pi[x]_{f(x)}$ 同构. 根据带余除法, 对于 $i=0,\ 1,\ 2,\ \cdots,\ p^n-2$,

$$x^i=q_i(x)f(x)+r_i(x), \quad 而\ \partial^0 r_i(x)<\partial^0 f(x).$$

将 $x=\xi$ 代入上式得

$$\xi^i=r_i(\xi)\in F_0, \quad i=0,\ 1,\ 2,\ \cdots,\ p^n-2.$$

但

$$F^*=\{\xi^0=e,\ \xi^1=\xi,\ \xi^2,\ \cdots,\ \xi^{p^n-2}\}.$$

因此 $F^*\subset F_0$. 又显然 $0\in F_0$. 所以 $F=F_0$. 由此推出 $\partial^0 f(x)=n$.

写

$$f(x)=f_0+f_1x+f_2x^2+\cdots+f_{n-1}x^{n-1}+x^n,\ f_i\in\Pi.$$

令

$$g(x)=f'_0+f'_1x+f'_2x^2+\cdots+f'_{n-1}x^{n-1}+x^n,\ f'_i\in\Pi',$$

其中 f'_i 表 f_i 在同构映射 σ 之下的象, 即

$$\sigma(f_i)=f'_i, \quad i=0,\ 1,\ 2,\ \cdots,\ n-1.$$

因 $f(x)$ 是 Π 上的不可约多项式, 易证 $g(x)$ 是 Π' 上的不可约多项式. 但 $\partial^0 g(x)=n$, 所以根据引理 2 有

$$g(x)\mid x^{p^n}-x.$$

根据引理 1, F' 中的 p^n 个元素都是 $x^{p^n}-x$ 的根. 再利用 §2

定理 5 的系理 2 就知道，F' 中的 p^n 个元素就是 $x^{p^n}-x$ 的全部根。因此 F' 中一定有一个元素 ξ' 适合 $g(x)$。因 $g(x)$ 是首项系数为 e 的 Π' 上的不可约多项式，所以 $g(x)$ 就是 ξ' 在 Π' 上的极小多项式。根据引理 9 就推出

$$F'=\{a_0'+a_1'\xi'+a_2'\xi'^2+\cdots+a_{n-1}'\xi'^{n-1}\\ \mid a_0', a_1', a_2', \cdots, a_{n-1}'\in\Pi'\},$$

而 F' 与 $\Pi'[x]_{g(x)}$ 同构。

易证，映射

$$\sum_{i=0}^{n-1}a_ix^i\to\sum_{i=0}^{n-1}\sigma(a_i)x^i\quad(a_i\in\Pi)$$

是从 $\Pi[x]_{f(x)}$ 到 $\Pi'[x]_{g(x)}$ 的一个同构对应，因此 $\Pi[x]_{f(x)}$ 与 $\Pi'[x]_{g(x)}$ 同构。从 F 与 $\Pi[x]_{f(x)}$ 同构，$\Pi[x]_{g(x)}$ 与 $\Pi'[x]_{g(x)}$ 同构，以及 $\Pi'[x]_{g(x)}$ 与 F' 同构，即可推出 F 与 F' 同构。当然也可以直接验证，映射

$$\sum_{i=0}^{n-1}a_i\xi^i\to\sum_{i=0}^{n-1}\sigma(a_i)\xi'^i\quad(a_i\in\Pi)$$

是从 F 到 F' 的一个同构对应。

这样定理 3 就证明了。

定理 3 是说，对于任意素数 p 和任意正整数 n，"基本上"有唯一的一个含有 p^n 个元素的有限域。今后我们总是用 $\mathbf{F}_{p^n}$ 来代表这个 p^n 个元素的有限域，并把它的单位元素记作 1. 为了具体造出 $\mathbf{F}_{p^n}$，需要具体求出 p 个元素的有限域 $\mathbf{F}_p$ 上的 n 次不可约多项式，这个问题将在第五章中讨论。值得注意的是，如果 $f(x)$ 和 $g(x)$ 是 $\mathbf{F}_p$ 上两个不同的 n 次不可约多项式，$\mathbf{F}_p[x]_{f(x)}$ 和 $\mathbf{F}_p[x]_{g(x)}$ 都是 p^n 个元素的有限域；根据定理 3，它们是同构的，因此可以把它们看作同一个 $\mathbf{F}_{p^n}$。

作为本节证明的有限域的结构定理的应用，我们证明

定理 6 设 $\mathbf{F}_{p^n}$ 是 p^n 个元素的有限域，而 $\mathbf{F}_p$ 是它的素

域. 如果 F_0 是 $\mathbf{F}_{p^n}$ 的子域, 可以假定 F_0 含 p^m 个元素, 那么 m 一定是 n 的因数. 反之, 如果 m 是 n 的因数, 那么 $\mathbf{F}_{p^n}$ 有唯一的一个含 p^m 个元素的子域. 更进一步, 设 $\mathbf{F}_{p^m}$ 和 $\mathbf{F}_{p^{m'}}$ 都是 $\mathbf{F}_{p^n}$ 的子域, 那么 $\mathbf{F}_{p^m}\subset\mathbf{F}_{p^{m'}}$, 当且仅当 m 是 m' 的因数.

证. 设 F_0 是 $\mathbf{F}_{p^n}$ 的子域. 因 F_0 包有 $\mathbf{F}_{p^n}$ 的单位元素 1, 所以包有 $\mathbf{F}_{p^n}$ 的素域 $\mathbf{F}_p$ 作为它自己的素域. 那么根据定理 1 可设 F_0 含 p^m 个元素. 又因 $\mathbf{F}_{p^n}$ 包有含 p^m 个元素的域 F_0 作为子域, 根据定理 4, $p^n=(p^m)^k$. 因此 $n=mk$, 这就是说, m 是 n 的因数.

反之, 设 m 是 n 的因数. 因 $\mathbf{F}_{p^n}$ 的 p^n 个元素恰好是多项式

$$x^{p^n}-x$$

的 p^n 个根, 而

$$x^{p^m}-x\,|\,x^{p^n}-x.$$

所以 $\mathbf{F}_{p^n}$ 中恰好有 p^m 个元素是多项式

$$x^{p^m}-x$$

的根. 用 F_0 表 $x^{p^m}-x$ 在 $\mathbf{F}_{p^n}$ 中的 p^m 个根所组成的集合. 设 $\alpha,\ \beta\in F_0$, 即

$$\alpha^{p^m}=\alpha,\ \beta^{p^m}=\beta.$$

那么

$$(\alpha+\beta)^{p^m}=\alpha^{p^m}+\beta^{p^m}=\alpha+\beta,$$

$$(\alpha\beta)^{p^m}=\alpha^{p^m}\cdot\beta^{p^m}=\alpha\beta,$$

因此 $\alpha+\beta,\ \alpha\beta\in F_0$, 即 F_0 对于 $\mathbf{F}_{p^n}$ 中的加法运算和乘法运算是自封的. 显然 $0,\ 1\in F_0$. 仍设 $\alpha\in F_0$, 那么

$$(-\alpha)^{p^m}=(-1)^{p^m}\alpha^{p^m}=-\alpha,$$

而当 $\alpha\neq0$ 时,

$$(\alpha^{-1})^{p^m}=(\alpha^{p^m})^{-1}=\alpha^{-1}.$$

因此 $-\alpha\in F_0$, 而当 $\alpha\neq0$ 时, $\alpha^{-1}\in F_0$. 这证明 F_0 是 $\mathbf{F}_{p^n}$ 的子域, 而根据 F_0 的定义可知它含 p^m 个元素.

如果 F_1 是 $\mathbf{F}_{p^n}$ 的另一个含 p^m 个元素的子域. 那么 F_1

的 p^m 个元素也是多项式

$$x^{p^m}-x$$

的 p^m 个根. 但 $x^{p^m}-x$ 在 $\mathbf{F}_{p^n}$ 中顶多有 p^m 个根, 因此 $F_1=F_0$.

更进一步, 设 $\mathbf{F}_{p^m}$ 和 $\mathbf{F}_{p^{m'}}$ 都是 $\mathbf{F}_{p^n}$ 的子域. 如果 $\mathbf{F}_{p^m}\subset\mathbf{F}_{p^{m'}}$, 那么根据定理 4, $p^{m'}=(p^m)^l$, 因此 m 是 m' 的因数. 反之, 如果 m 是 m' 的因数, 那么 $\mathbf{F}_{p^{m'}}$ 就包有一个含 p^m 个元素的子域 F_0, 它也是 $\mathbf{F}_{p^n}$ 的子域. 但 $\mathbf{F}_{p^n}$ 只有唯一的一个含 p^m 个元素的子域 $\mathbf{F}_{p^m}$. 因此 $F_0=\mathbf{F}_{p^m}$. 于是 $\mathbf{F}_{p^m}\subset\mathbf{F}_{p^{m'}}$.

这样定理 6 就完全证明了.

最后我们再对极小多项式作进一步的探讨.

定理 7 设 F 是个有限域, $\mathbf{F}_q$ 是它的一个恰含 q 个元素的子域, 而 α 是 F^* 中任一元素. 假定 α 在 F^* 中的阶是 l, 那么 $(q, l)=1$. 再假定 $(q)_l$ 在 $\mathbf{Z}_l^*$ 中的阶是 m, 那么 α 在 F_q 上的极小多项式 $f(x)$ 就是 m 次的, $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$ 就是 $f(x)$ 的 m 个两两不同的根, 而且它们在 F^* 中的阶都是 l. 更进一步, 如果再假定 F 的元素个数是 q^n, 那么 F 中本原元在 $\mathbf{F}_q$ 上的极小多项式一定是 n 次的, 它的 n 个根都是 F 的本原元.

证. 设 α 是 F^* 中任一元素, 并假定 α 在 F^* 中的阶是 l. 根据引理 1, $\alpha^{q^n-1}=e$. 那么根据 §4 定理 4, $l\,|\,q^n-1$. 但是 $(q^n-1, q)=1$, 因此 $(q, l)=1$. 于是 $((q)_l, l)=1$, 那么 $(q)_l\in\mathbf{Z}_l^*$.

将 α 在 $\mathbf{F}_q$ 上的极小多项式 $f(x)$ 写成

$$f(x)=a_0+a_1x+a_2x^2+\cdots+x^k,\ a_i\varepsilon\mathbf{F}_q.$$

那么 $$f(\alpha)=a_0+a_1\alpha+a_2\alpha^2+\cdots+\alpha^k=0.$$

因 q 是 F 的特征的幂, 根据 §3 定理 5 诸系理, 以及本节引理 1,

$$\begin{aligned}0=f(\alpha)^q&=a_0^q+a_1^q\alpha^q+a_2^q(\alpha^2)^q+\cdots+(\alpha^k)^q\\&=a_0+a_1\alpha^q+a_2(\alpha^q)^2+\cdots+(\alpha^q)^k.\end{aligned}$$

这就是说，α^q 也是 $f(x)$ 的一个根. 同理可证，α^{q^2}, α^{q^3}, $\cdots$ 都是 $f(x)$ 的根.

再设 $(q)_l$ 在 $\mathbf{Z}_l^*$ 中的阶是 m, 那么 $(q)_l^m=1$, 于是 $l\mid q^m-1$. 因此

$$\alpha^{q^m}=\alpha.$$

我们再证明 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$ 这 m 个元素两两不同. 假定 $\alpha^{q^i}=\alpha^{q^j}$, $0\leqslant i\leqslant j\leqslant m-1$, 那么 $\alpha^{q^j-q^i}=1$. 于是 $l\mid q^j-q^i$. 因 $(l, q)=1$, 所以 $l\mid q^{j-i}-1$, 即 $(q^{j-i}-1)_l=0$. 因此 $(q)_l^{j-i}=1$. 那么 $m\mid j-i$. 但 $0\leqslant i\leqslant j\leqslant m-1$, 所以 $i=j$. 这证明了

$$\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$$

这 m 个元素是 $f(x)$ 的 m 个两两不同的根.

令

$$g(x)=(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\cdots(x-\alpha^{q^{m-1}}).$$

将 $g(x)$ 写成

$$g(x)=b_0+b_1x+b_2x^2+\cdots+b_mx^m,$$

其中
$$b_i=g_i(\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}})\in F,$$

而 $g_i(x_0, x_1, x_2, \cdots, x_{m-1})$ 是 $\mathbf{F}_q$ 上(实际上是 $\mathbf{F}_q$ 的素域上)的 m 个文字 $x_0, x_1, x_2, \cdots, x_{m-1}$ 的多项式. 因 $\alpha^{q^m}=\alpha$, 所以

$$g(x)=(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})\cdots(x-\alpha^{q^m}),$$

于是对 $i=0, 1, 2, \cdots, m$, 有

$$\begin{aligned}b_i&=g_i(\alpha^q, \alpha^{q^2}, \alpha^{q^3}, \cdots, \alpha^{q^{m-1}}, \alpha^{q^m})\\&=[g_i(\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-2}}, \alpha^{q^{m-1}})]^q=b_i^q.\end{aligned}$$

再根据引理 1, $b_i\in\mathbf{F}_q$ 对一切 i. 这证明了 $g(x)\in F_q[x]$. 又因 $g(x)$ 的根都是 $f(x)$ 的根, 所以 $g(x)\mid f(x)$. 但根据引理 8, $f(x)$ 不可约. 因此 $g(x)=f(x)$. 这证明了 $f(x)$ 是 m 次的, 而 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$ 是它的 m 个两两不同的根. 又因 $(q, l)=1$, 所以根据 § 4 引理 1 可知, 对任意 $i=0, 1, 2, \cdots, m-1$, α^{q^i} 都是 F^* 中的 l 阶元素.

最后, 再假定 F 的元素个数是 q^n, 那么 F 中本原元都

是q^n-1阶的．显然q在$\mathbf{Z}_{q^n-1}^*$中的阶是n．因此F中本原元的极小多项式一定是n次的，而它的n个根都是F^*中q^n-1阶元素，即都是F中的本原元．

这样定理7就完全证明了．

系理1 设q是一个素数的幂，而$\mathbf{F}_q$是q个元素的有限域，再设$f(x)$是$\mathbf{F}_q$上的一个n次不可约多项式，并假定$f(x)\neq x$，可以把$\mathbf{F}_q$看成$\mathbf{F}_{q^n}$的子域，譬如取$\mathbf{F}_{q^n}=\mathbf{F}_q[x]_{f(x)}$即可，那么$f(x)$的$n$个根都在$\mathbf{F}_{q^n}$中，而且它们在$\mathbf{F}_{q^n}^*$中有相同的阶．

证．根据引理2

$$f(x)\mid x^{q^n}-x.$$

再根据引理1，$\mathbf{F}_{q^n}$的q^n个元素就是多项式$x^{q^n}-x$的q^n个根．因此$f(x)$的n个根都在$\mathbf{F}_{q^n}$中．因$f(x)$不可约，而$f(x)\neq x$，所以

$$f(x)\mid x^{q^n-1}-1.$$

因此$f(x)$的n个根都是$x^{q^n-1}-1$的根，于是都属于$\mathbf{F}_{q^n}^*$．仍因$f(x)$不可约，所以它是它的任意一个根在$\mathbf{F}_q$上的极小多项式，那么从定理7就可以推出$f(x)$的n个根在$\mathbf{F}_{q^n}^*$中有相同的阶．

基于这个系理，我们可以给出下面这个定义

定义2 设q是一个素数的幂．$f(x)$是$\mathbf{F}_q$上的一个n次不可约多项式，而$f(x)\neq x$．$f(x)$的周期定义为$f(x)$在$\mathbf{F}_{q^n}$中的n个根在$\mathbf{F}_{q^n}^*$中的公共的阶．$f(x)$的指数定义为用它的周期去除q^n-1所得的商．如果$f(x)$的周期是q^n-1，那么$f(x)$就叫做$\mathbf{F}_q$上的**本原多项式**．换句话说，如果$f(x)$的根都是$\mathbf{F}_{q^n}$的本原元，那么$f(x)$就叫做本原多项式．

系理2 设q是一个素数的幂，$f(x)$是$\mathbf{F}_q$上的一个n次不可约多项式而$f(x)\neq x$，那么$f(x)$的周期就是x在群

$\mathbf{F}_q[x]^*_{f(x)}$ 中的阶，而 $f(x)$ 的指数就等于 $|F_q[x]^*_{f(x)}|/|[x]|$.

证. 这是因为 x 就是 $f(X)$ 在 q^n 个元素的域 $\mathbf{F}_q[x]_{f(x)}$ 中的一个根

定义 3 设

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$

是 $\mathbf{F}_q$ 上的一个 n 次多项式，而 $a_0a_n\neq0$. 我们把

$$\tilde{f}(x)=x^nf\left(\frac{1}{x}\right)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n$$

叫做与 $f(x)$ 互反的多项式.

显然有

i) $\tilde{\tilde{f}}(x)=f(x)$,

ii) $f(x)$ 和 $\tilde{f}(x)$ 同时是可约多项式或不可约多项式.

iii) 当 $f(x)$ 和 $\tilde{f}(x)$ 同时是不可约多项式时，设 $\alpha(\in\mathbf{F}_{q^n})$ 是 $f(x)$ 的一个根，那么 $\alpha^{-1}(\in\mathbf{F}_{q^n})$ 就是 $\tilde{f}(x)$ 的一个根. 因 α 和 α^{-1} 在 $\mathbf{F}^*_{q^n}$ 中有相同的阶，所以 $f(x)$ 和 $\tilde{f}(x)$ 的周期相等.

iv) $f(x)$ 和 $\tilde{f}(x)$ 同时是本原多项式或不是本原多项式.

一般说来，不可约多项式不一定是本原多项式. 例如 $\mathbf{F}_3$ 上的不可约多项式 x^2+1 在 $\mathbf{F}_{3^2}=\mathbf{F}_3[x]_{x^2+1}$ 中有两个根 x 和 $-x$，而

$$(\pm x)^4=(-1)^2=1.$$

因 $4\neq3^2-1$，所以 x^2+1 不是本原多项式. 又如，$\mathbf{F}_2$ 上的多项式 $f(x)=x^4+x^3+x^2+x+1$ 是不可约的，因为易证它不被 $\mathbf{F}_2$ 上的 1 次多项式 x, $x+1$ 和 $\mathbf{F}_2$ 上唯一的 2 次不可约多项式 x^2+x+1 所整除. 但 $f(x)$ 在 $\mathbf{F}_2[x]_{f(x)}$ 中的根 x 在 $\mathbf{F}_2[x]^*_{f(x)}$ 中的阶是 5,

$$x^5-1=(x-1)(x^4+x^3+x^2+x+1)=0,$$

而 $5\neq2^4-1$，所以 $f(x)$ 也不是本原多项式.

但是，我们有

定理 8 设 q 是一个素数的幂，而 n 是任意一个正整数，那么 $\mathbf{F}_q$ 上一定有 n 次本原多项式存在. 更进一步，$\mathbf{F}_q$ 上首项系数为 1 的 n 次本原多项式的个数是 $\varphi(q^n-1)/n$.

证. 根据 § 4 定理 5，$\mathbf{F}_{q^n}$ 一定有本原元. 设 ξ 是 $\mathbf{F}_{q^n}$ 的一个本原元. 那么根据定理 7，ξ 在 $\mathbf{F}_q$ 上的极小多项式是 n 次的而且它的根都是 $\mathbf{F}_{q^n}$ 的本原元. 因此 ξ 在 $\mathbf{F}_q$ 上的极小多项式就是 n 次本原多项式.

更进一步，设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个首项系数为 1 的 n 次本原多项式，那么 $f(x)$ 的根都是 $\mathbf{F}_{q^n}$ 的本原元. 再设 $g(x)$ 也是 $\mathbf{F}_q$ 上的一个首项系数为 1 的 n 次本原多项式. 如果 $f(x)$ 和 $g(x)$ 在 $\mathbf{F}_{q^n}$ 中有一个公根 ξ，那么 $f(x)$ 和 $g(x)$ 都是 ξ 的极小多项式. 根据引理 8，$f(x)=g(x)$. 因此 $\mathbf{F}_q$ 上首项系数为 1 的 n 次本原多项式的个数乘以 n（每一个 n 次本原多项式在 $\mathbf{F}_{q^n}$ 中根的个数）就等于 $\mathbf{F}_{q^n}$ 的本原元的个数 $\varphi(q^n-1)$. 所以 $\mathbf{F}_q$ 上首项系数为 1 的 n 次本原多项式的个数等于 $\varphi(q^n-1)/n$.

定理 9 设 q 是一个素数的幂而 n 是一个正整数，并设 q^n-1 是素数. 如果 q 是奇数，那么一定有 $q=3$ 而 $n=1$. 如果 $q=2$，那么 n 一定是素数. 特别，当 2^n-1 是素数时，$\mathbf{F}_2$ 上的 n 次不可约多项式一定是 n 次本原多项式.

证. 先设 q 是奇素数的幂，那么 $q-1$ 就是偶数. 但显然有

$$q-1 \mid q^n-1,$$

因此 2 是 q^n-1 的一个因数. 当 $q>3$ 时或当 $q=3$ 而 $n>1$ 时，我们有 $2<q^n-1$. 因此这时 q^n-1 不是素数. 我们证明了，当 q 是奇素数的幂时，如果 q^n-1 是素数，一定有 $q=3$ 而 $n=1$.

再设 $q=2$. 如果 n 不是素数而 $n>1$, 设 m 是 n 的一个因数而 $1<m<n$, 那么

$$2^m-1 \mid 2^n-1,$$

因此 2^m-1 是 2^n-1 的因数而 $1<2^m-1<2^n-1$. 因此 2^n-1 不是素数. 如果 $n=1$, $2^n-1=2^1-1=1$ 也不是素数. 这证明了, 当 2^n-1 是素数时, n 一定是素数.

当 2^n-1 是素数时, $\mathbf{F}_{2^n}^*$ 中 $\neq 1$ 的元素的阶都是 2^n-1, 即 $\mathbf{F}_{2^n}^*$ 中 $\neq 1$ 的元素都是 $\mathbf{F}_{2^n}$ 的本原元. 这时 $x^{2^n-1}-1$ 在 $\mathbf{F}_2$ 上的 $\neq x-1$ 的不可约因式就都是 $\mathbf{F}_{2^n}$ 中本原元的极小多项式, 因而都是 $\mathbf{F}_2$ 上的 n 次本原多项式. 但当 2^n-1 是素数时, n 一定是素数, 因此 $n>1$. 于是 $\mathbf{F}_2$ 上的 n 次不可约多项式就都是 $x^{2^n-1}-1$ 的 $\neq x-1$ 的不可约因式, 所以都是 n 次本原多项式. 定理 9 就证完了.

从定理 9 可知, 讨论 2^n-1 何时是素数是有意义的. 但即使 n 是素数, 2^n-1 仍可能是复合数. 例如 $2^{11}-1=2047=23\times 89$. 当 p 是素数, 而 2^p-1 也是素数时, 2^p-1 就叫 Mersenne 素数. 令

$$M_p=2^p-1.$$

目前已知的 Mersenne 素数一共 27 个, 即当

$p=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107,$
$127, 521, 607, 1279, 2203, 2281, 3217,$
$4253, 4423, 9689, 9941, 11213, 19937, 21701,$
$44497, 86243$ 时, M_p 是素数.

§6 交换环和理想

在 §1 里我们引进了域的概念. 在前面几节里我们也看到了域的概念概括了常见的有理数域 $\mathbf{Q}$, 实数域 $\mathbf{R}$, 复数域

$\mathbf{C}$以及含任一素数 p 的幂 p^n 个元素的有限域 $\mathbf{F}_{p^n}$. 但是域的概念却不能概括另一些常见的代数结构，如全体整数所组成的集合 $\mathbf{Z}$, 域 F 上一个文字 x 的多项式的全体所组成的集合 $F[x]$ 等. 又如当 m 是复合数时，$\mathbf{Z}_m$ 对于模 m 加法和模 m 乘法来说也不是域. 我们也知道 $\mathbf{Z}$, $F[x]$ 和 $\mathbf{Z}_m$(m 是复合数)这些代数结构里都规定了加法和乘法运算，它们对于它们里面规定的加法和乘法运算都是自封的，而且它们的加法和乘法运算满足域的公理 I, II.1, II.2, II.3 和 III, 但是 II.4 并不成立. 为了能概括 $\mathbf{Z}$, $F[x]$ 和 $\mathbf{Z}_m$(m 是复合数)这些代数结构以及更广的一些代数结构，我们需要引进交换环的概念.

定义 1 设 R 是一个非空集合. 假定在 R 中规定了加法和乘法这两种运算，并假定 R 对于这两种运算都是自封的. 我们说 R 对于所规定的加法运算和乘法运算是一个 交 换 环，如果以下运算规则成立:

I R 对于加法运算是一个交换群.

II.1 对任意 $a, b\in R$, 有

$$ab=ba.$$

II.2 对任意 $a, b, c\in R$, 有

$$(ab)c=a(bc).$$

III 对任意 $a, b, c\in R$, 有

$$a(b+c)=ab+ac.$$

根据以前的讨论，我们知道 $\mathbf{Z}$, $F[x]$, $F[x_1, x_2, \cdots, x_n]$ 和 $\mathbf{Z}_m$ 都是交换环，它们分别叫做整数环，域 F 上一个文字 x 的多项式环，域 F 上 n 个文字 $x_1, x_2, \cdots, x_n$ 的多项式环和整数模 m 的环. 我们再举一个交换环的例子，它对于编码来说是重要的.

例 1 设 F 是一个域，$f(x)$ 是 $F[x]$ 中的一个 n 次多项式，它不一定是不可约的. 令

$$F[x]_{f(x)}=\{a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}|a_i\in F\},$$

在 $F[x]_{f(x)}$ 中引进加法和乘法.对任意 $a(x)$, $b(x)\in F[x]_{f(x)}$,规定

$$a(x)\oplus b(x)=a(x)+b(x),$$
$$a(x)\odot b(x)=(a(x)b(x))_{f(x)}.$$

并把它们分别称为模 $f(x)$ 的加法和模 $f(x)$ 的乘法. 那么可以验证 $F[x]_{f(x)}$ 对于如上规定的加法运算和乘法运算是一个交换环,叫做域 F 上一个文字 x 的多项式模 $f(x)$ 的环.

我们附带说一下,环是抽象代数的基本概念之一,有许多重要应用. 在定义 1 中把运算规则 II.1 取消, 就得到环的定义. 但本书中我们只讨论交换环.

定义 2 设 R 是一个交换环. 我们知道 R 对于其中的加法运算是一个交换群, 叫做 R 的*加法群*. R 的加法群的单位元素叫做 R 的*零元素*, 记作 0. R 中任一元素 a 在 R 的加法群中的逆元素叫做 a 的*负元素*, 记作 $-a$. 如果 R 中有唯一的一个 $\neq 0$ 的元素 e, 具有性质 $ae=a$ 对任意 $a\in R$, 那么 e 就叫做 R 的*单位元素*, 而 R 叫做*有单位元素的交换环*. 今后我们总把有单位元素的交换环中的单位元素记作 1.

完全和 § 1 定理 1 中的 iii) 一样, 可以证明, 如果交换环 R 中有一个 $\neq 0$ 的元素 e, 具有性质 $a\cdot e=a$ 对任意 $a\in R$, 那么 e 是唯一确定的,因而是 R 的单位元素 1.

我们知道, $\mathbf{Z}$, $F[x]$, $F[x_1, x_2, \cdots, x_n]$, $\mathbf{Z}_m$ 和 $F[x]_{f(x)}$ 都是有单位元素的交换环.

仔细检查一下 § 1 定理 2 中 i) 和 iii) 的证明就会发现并没有用到域的公理 II.3 和 II.4, 因此我们有

定理 1 设 R 是交换环, 那么 R 中的加法运算和乘法运算还满足下面的运算规则:

i) (*加法消去律*)设 a, b, c 是 R 中任意三个元素. 如果

$a+c=b+c$, 那么 $a=b$.

ii) $a\cdot 0=0$, 对任意 $a\in R$.

但是在一个交换环中，乘法消去律却不一定成立. 譬如，当 m 是复合数时，$\mathbf{Z}_m$ 中就是如此. 设 $m=m_1m_2, 1<m_1, m_2<m$, 那么 $m_1, m_2\in\mathbf{Z}_m$. 但是

$$m_1\odot m_2=(m_1m_2)_m=(m)_m=0$$

显然

$$m_1\odot 0=0.$$

因此

$$m_1\odot m_2=m_1\odot 0,$$

而

$$m_1\neq 0,\quad m_2\neq 0.$$

定义 3 设 R 是个交换环. 如果在 R 中乘法消去律成立，即对任意 $a, b, c\in R$ 而 $c\neq 0$, 从 $a\cdot c=b\cdot c$ 可推出 $a=b$, 我们就说 R 是个交换整环.

容易证明，$\mathbf{Z}$, $F[x]$, $F[x_1, x_2, \cdots, x_n]$ 都是交换整环. 但当 m 是复合数时，$\mathbf{Z}_m$ 却不是交换整环. 同理可证，当 $f(x)$ 是 $F[x]$ 中的可约多项式时，$F[x]_{f(x)}$ 也不是交换整环.

定义 4 设 R 是一个交换环，再设 a, b 是 R 中两个 $\neq 0$ 的元素. 如果 $ab=0$, 我们就说 a, b 是 R 的零因子. 如果 R 没有零因子，我们就说 R 是无零因子的交换环.

定理 2 设 R 是个交换环，那么 R 是交换整环，当且仅当 R 没有零因子，即 R 是无零因子的交换环.

证. 先假定 R 是交换整环. 设 $a, b\in R$ 而 $ab=0$. 如果 $a\neq 0$, 根据定理 1 中的 ii) 有 $a\cdot 0=0$. 那么根据乘法消去律，从 $ab=a0$ 推出 $b=0$. 因此 R 不可能有零因子.

反过来，设 R 是无零因子的交换环，设 $a, b, c\in R$, $c\neq 0$ 而 $ac=bc$, 那么 $(a-b)c=ac-bc=0$. 因为 R 没有零因子，所以 $a-b=0$, 于是 $a=b$. 这证明了 R 中乘法消去律成立. 因此 R 是交换整环.

自然我们也可以利用交换环 R 中的负元素来定义 R 中的

减法. 即如果 $a,\ b\in R$, 定义

$$a-b=a+(-b).$$

也可以证明 R 中的加法、减法和乘法运算满足 §1 里所举出来的某些运算规则，我们就不重复了.

平行于域的子域、交换群的子群，我们可以定义交换环的子环这个概念.

定义 5 设 R 是一个交换环，而 R_0 是 R 的一个非空子集. 如果 R_0 对于 R 中的加法和乘法运算也是一个交换环，我们就说 R_0 是 R 的子环.

显然，当需要验证交换环 R 的一个子集 R_0 是子环时，除了要验证 R_0 对于 R 中的加法和乘法运算是自封的以外，只需要验证 R_0 是 R 的加法群的一个子群即可. 因 II.1, II.2 和 III 在 R_0 中自然成立.

我们举一个子环的例子.

例 2 设 m 是个整数. 用 $m\mathbf{Z}$ 表示 m 的所有整数倍数所组成的集合，即

$$m\mathbf{Z}=\{mn\mid n\in\mathbf{Z}\}.$$

因

$$mn_1+mn_2=m(n_1+n_2)$$

$$(mn_1)\cdot(mn_2)=m(mn_1n_2)$$

所以 $m\mathbf{Z}$ 对于 $\mathbf{Z}$ 中加法和乘法运算是自封的. 又因 $0=m\cdot 0\in m\mathbf{Z}$, 而 $m\mathbf{Z}$ 中任一元素 mn 的负元素 $-mn=m(-n)\in m\mathbf{Z}$, 所以 $m\mathbf{Z}$ 对于 $\mathbf{Z}$ 中加法运算是一个子群. 这证明了 $m\mathbf{Z}$ 是 $\mathbf{Z}$ 的子环.

我们注意，当 $m\neq\pm1$ 时，$m\mathbf{Z}$ 是没有单位元素的环.

我们再注意，如果 $mn\in m\mathbf{Z}$, 而 k 是 $\mathbf{Z}$ 中任意元素，那么

$$k(mn)=m(kn)\in m\mathbf{Z}.$$

这建议我们给出以下定义.

定义 6 设 R 是一个交换环，而 R_0 是 R 的一个子环. 如

果 R_0 具有性质：对任意 $a\in R_0$ 和 $r\in R$，都有 $ra\in R_0$，那么我们就把 R_0 叫做 R 的一个理想.

根据这个定义和上面的分析，我们可以说，对任意整数 m，$m\mathbf{Z}$ 都是 $\mathbf{Z}$ 的理想. 一般地，我们有

定理 3 设 R 是一个交换环，而 a 是 R 中任意一个元素. 那么

$$(a)=\{ra \mid r\in R\}$$

就是 R 的一个理想.

为了证明这个定理，我们先给出交换环的一个非空子集是它的理想的一个充要条件. 这个条件使我们验证交换环的一个非空子集是理想时比较简单.

定理 4 设 R 是个交换环. R 的一个非空子集 I 是 R 的一个理想，当且仅当以下二条件成立.

1) 对任意 $a, b\in I$，都有 $a-b\in I$.

2) 对任意 $a\in I$ 和 $r\in R$，都有 $ra\in I$.

证. 先设 R 是 I 的理想，那么对任意 $a, b\in I$，由于 I 是 R 的加法群的子群，所以 $a-b=a+(-b)\in I$，这证明了 1) 成立. 根据定义 6, 2) 当然成立.

其次设 I 是 R 的非空子集，而 1) 和 2) 成立. 我们来证明 I 是 R 的理想. 这只要证明 I 是 R 的子环就行了，而这只要证明 I 是 R 的加法群的子群就行了. 设 a 是 I 中任一元素，那么根据 1)，$0=a-a\in I$. 仍根据 1)，$-a=0-a\in I$. 这证明了 I 是 R 的加法群的子群. 因此 I 是 R 的理想.

现在回头去证明定理 3. 设 R 是个交换环而 $a\in R$. 对 (a) 中任意两个元素 $r'a$, $r''a$ $(r', r''\in R)$，我们有

$$r'a-r''a=(r'-r'')a.$$

因 R 是交换环，$r-r'\in R$，因此 $(r-r')a\in(a)$. 这证明了定理 4 中的条件 1) 成立. 再设 r 是 R 中任一元素，那么

$$r(r'a)=(rr')a.$$

因 R 是交换环，$rr'\in R$，因此 $(rr')a\in R$，这证明了定理 4 中的条件 2) 成立．那么根据定理 4，知道(a)是R的理想．

基于定理 3，我们给出下面这个定义．

定义 7 设 R 是个交换环，而 a 是 R 中任意一个元素，那么(a)就叫做由 a 生成的理想．

特别，对任意整数 m，$m\mathbf{Z}$ 就是由m生成的理想(m)．反过来，我们有

定理 5 $\mathbf{Z}$ 的任一理想都是由某一整数 m 生成的理想 $m\mathbf{Z}$．实际上，$\mathbf{Z}$ 的任一理想都是它所含的最小非负整数所生成的理想．更进一步，$m\mathbf{Z}=m'\mathbf{Z}$，当且仅当 $m=\pm m'$．

证．设 I 是 $\mathbf{Z}$ 的一个理想．用(0)表示仅由 0 这唯一的一个数所组成的理想．如果 $I=(0)$，那么 $I=0\mathbf{Z}$．如果 $I\neq(0)$，那么 I 中就有一个 $\neq 0$ 的整数 a．如果 $a>0$，I 就包含一个正整数．如果 $a<0$，那么 $-a=0-a\in I$ 而 $-a>0$．因此 I 总包含一个正整数．设m是 I 所含的最小的正整数，那么根据定义 6 显然有 $m\mathbf{Z}\subset I$．更进一步，设 n 是 I 中任一元素．根据带余除法，可以写

$$n=qm+(n)_m,\quad 0\leqslant(n)_m<m,$$

那么 $qm\in I$，于是

$$(n)_m=n-qm\in I.$$

因为m是 I 所含的最小正整数，所以$(n)_m=0$．于是 $n=qm\in m\mathbf{Z}$，因此 $I\subset m\mathbf{Z}$．这证明了 $I=m\mathbf{Z}$．

显然 $m\mathbf{Z}=(-m)\mathbf{Z}$．又设 $m\mathbf{Z}=m'\mathbf{Z}$，那么m是 m' 的倍数而 m' 也是m的倍数．因此 $m=\pm m'$．

这样定理 5 就完全证明了．

定理 5 有下面这个应用．

系理 设 $m_1, m_2, \cdots, m_r$ 是 r 个 $\neq 0$ 的整数，并设 d 是它

们的最大公因数，那么一定可以找到 r 个整数 $c_1, c_2, \cdots, c_r$ 使

$$d=c_1m_1+c_2m_2+\cdots+c_rm_r.$$

证．令

$$I=\{a_1m_1+a_2m_2+\cdots+a_rm_r \mid a_i\in\mathbf{Z}\}.$$

容易验证 I 是 $\mathbf{Z}$ 的一个理想．根据定理 5，I 就是由它所含的最小正整数 m 所生成的理想 $m\mathbf{Z}$，即 $I=m\mathbf{Z}$.

因 $m_1, m_2, \cdots, m_r\in I$，所以

$$m\mid m_1,\ m\mid m_2,\ \cdots,\ m\mid m_r,$$

即 m 是 $m_1, m_2, \cdots, m_r$ 的公因数，因此 $m\leqslant d$.

另一方面，$m\in I$．因此有 $c_i\in\mathbf{Z}$ 使

$$m=c_1m_1+c_2m_2+\cdots+c_rm_r.$$

那么从

$$d\mid m_1,\ d\mid m_2,\ \cdots,\ d\mid m_r$$

推出 $d\mid m$．因此 $d\leqslant m$．所以 $d=m$，而

$$d=c_1m_1+c_2m_2+\cdots+c_rm_r.$$

完全平行于定理 5，我们有

定理 6　设 F 是域，而 $f(x)$ 是 $F[x]$ 中的任一多项式．用 $(f(x))$ 表 $f(x)$ 的所有倍式所组成的集合，即

$$(f(x))=\{k(x)f(x) \mid k(x)\in F[x]\},$$

那么 $(f(x))$ 是 $F[x]$ 的理想．反过来，$F[x]$ 的任一理想都是由 $F[x]$ 中某一多项式的一切倍式所组成的理想 $(f(x))$．实际上，当这个理想不是仅由 0 组成的理想 (0) 时，可以取 $f(x)$ 为这个理想中 $\neq 0$ 的次数最低的首项系数等于 1 的多项式．更进一步，$(f(x))=(f_1(x))$，当且仅当 $f(x)=cf_1(x)$ 而 $c\in F^*$.

系理　设 F 是域，而 $f_1(x), f_2(x), \cdots, f_r(x)$ 是 $F[x]$ 中 r 个 $\neq 0$ 的多项式，再设 $d(x)$ 是它们的最高公因式，那么一定可以找到 r 个多项式 $c_1(x), c_2(x), \cdots, c_r(x)$ 使

$$d(x)=c_1(x)f_1(x)+c_2(x)f_2(x)+\cdots+c_r(x)f_r(x).$$

我们不去直接证明定理 6，而去证明它的下面这个推广．这个推广在编码理论中有重要应用．

定理7 设 F 是域，而 $f(x)$ 是 $F[x]$ 中的一个 n 次多项式，再设 I 是交换环 $F[x]_{f(x)}$ 中的一个 $\neq(0)$ 的理想，那么 I 有唯一的一个 $\neq 0$ 的次数最低的首项系数等于 1 的多项式 $g(x)$ 使

$$I=\{k(x)g(x)\mid \partial^0 k(x)\leqslant n-1-\partial^0 g(x)\},$$

而且 $g(x)$ 是 $f(x)$ 的因式．反之，设 $g(x)$ 是 $f(x)$ 的一个首项系数为 1 的因式，那么

$$I_1=\{k(x)g(x)\mid \partial^0 k(x)\leqslant n-1-\partial^0 g(x)\}$$

就是 $F[x]_{f(x)}$ 的一个理想，而且是由 $g(x)$ 生成的理想 $(g(x))$，$g(x)$ 是这个理想里次数最低的首项系数等于 1 的多项式．

证．设 I 是 $F[x]_{f(x)}$ 的一个理想，并假定 $I\neq(0)$．选 $g(x)$ 是 I 中 $\neq 0$ 的一个次数最低的首项系数等于 1 的多项式．如果 $g_1(x)$ 也是这样一个多项式，那么 $g(x)-g_1(x)\in I$ 而

$$\partial^0(g(x)-g_1(x))\leqslant\partial^0 g(x)-1.$$

如果 $g(x)-g_1(x)\neq 0$，将 $g(x)-g_1(x)$ 的首项系数的逆元素乘上 $g(x)-g_1(x)$，就得到 I 中一个 $\neq 0$ 的次数 $<\partial^0 g(x)$ 的首项系数等于 1 的多项式．这与 $g(x)$ 的选择相矛盾．因此 $g(x)-g_1(x)=0$，即 $g(x)=g_1(x)$．这证明了 $g(x)$ 是 I 中唯一的 $\neq 0$ 的次数最低的首项系数等于 1 的多项式．

因 I 是 $F[x]_{f(x)}$ 的理想，所以对任意 $k(x)\in F[x]_{f(x)}$ 而 $\partial^0 k(x)\leqslant n-1-\partial^0 g(x)$，总有

$$k(x)g(x)=k(x)\odot g(x)\in I.$$

设 $h(x)$ 是 I 中任一元素．根据带余除法，有

$$h(x)=q(x)g(x)+r(x),\ \partial^0 r(x)<\partial^0 g(x).$$

因 $\partial^0 h(x)<\partial^0 f(x)$，所以

$$\partial^0(q(x)\cdot g(x))=\partial^0 h(x)<\partial^0 f(x),$$

于是 $$h(x)=q(x)\odot g(x)\oplus r(x),$$

那么 $$r(x)=h(x)-q(x)\odot g(x)\in I.$$

但 $g(x)$ 是 I 中 $\neq 0$ 的次数最低的一个首项系数等于 1 的多项式，而 $\partial^0 r(x)<\partial^0 g(x)$. 如果 $r(x)\neq 0$，将 $r(x)$ 的首项系数的逆元素乘上 $r(x)$，就得到 I 中一个 $\neq 0$ 的次数 $<\partial^0 g(x)$ 的首项系数等于 1 的多项式. 因此一定有 $r(x)=0$. 于是

$$h(x)=q(x)\odot g(x)=q(x)g(x).$$

这证明了

$$I=\{k(x)g(x)\mid \partial^0 k(x)\leqslant n-1-\partial^0 g(x)\}.$$

再证明 $g(x)$ 是 $f(x)$ 的因式. 根据带余除法

$$f(x)=q_1(x)\cdot g(x)+r_1(x),\quad \partial^0 r_1(x)<\partial^0 g(x).$$

于是

$$r_1(x)=(-q_1(x)g(x))_{f(x)}=-q_1(x)\odot g(x)\in I.$$

仍因 $g(x)$ 是 I 中 $\neq 0$ 的次数最低的首项系数等于 1 的多项式，所以一定有 $r_1(x)=0$. 于是

$$f(x)=q_1(x)g(x).$$

这证明了 $g(x)$ 是 $f(x)$ 的因式. 定理 7 的第一部分就证明了.

反过来，设 $g(x)$ 是 $f(x)$ 的一个首项系数为 1 的因式，那么 $f(x)=g(x)h(x)$. 令

$$I_1=\{k(x)g(x)\mid \partial^0 k(x)\leqslant n-1-\partial^0 g(x)\}.$$

我们来证明 I_1 是 $F[x]_{f(x)}$ 的一个理想. 设 $a(x)$ 是 $F[x]_{f(x)}$ 中任一元素. 根据带余除法，可以写

$$a(x)=q_2(x)h(x)+r_2(x),\ \partial^0 r_2(x)<\partial^0 h(x),$$

那么

$$\begin{aligned}a(x)\odot g(x)&=(q_2(x)h(x)+r_2(x))\odot g(x)\\&=(q_2(x)h(x))\odot g(x)+r_2(x)\odot g(x)\\&=(q_2(x)h(x)g(x))_{f(x)}+(r_2(x)g(x))_{f(x)},\end{aligned}$$

因 $f(x)=g(x)h(x)$，所以

$$(q_2(x)h(x)g(x))_{f(x)}=0.$$

因
$$\partial^0(r_2(x)g(x))=\partial^0 r_2(x)+\partial^0 g(x)$$
$$<\partial^0 h(x)+\partial^0 g(x)=\partial^0 f(x)=n,$$

所以
$$(r_2(x)g(x))_{f(x)}=r_2(x)g(x).$$

这证明了
$$a(x)\odot g(x)=r_2(x)g(x)\in I_1.$$

于是
$$(g(x))\subset I_1,$$

这里 $(g(x))$ 是由 $g(x)$ 生成的理想. 显然又有

$$I_1\subset(g(x)),$$

因此
$$I_1=(g(x)).$$

这证明了 I_1 是由 $g(x)$ 生成的理想. 显然 $g(x)$ 是 I_1 中次数最低的首项系数等于 1 的多项式.

定理 7 就完全证明了.

在定理 7 中令 $f(x)=0$，并约定 $F[x]_0=F[x]$，就得出定理 6.

同在 §3 定义 2 中我们定义过域的同构一样，我们也可以定义环的同构.

定义 8 设 R 和 R' 是两个交换环. 我们说 R 和 R' 同构，如果有一个从 R 到 R' 的一一对应

$$\sigma: a\to\sigma(a)\,(a\in R,\ \sigma(a)\in R'),$$

使得
$$\sigma(a+b)=\sigma(a)+\sigma(b),$$
$$\sigma(ab)=\sigma(a)\cdot\sigma(b).$$

这时 σ 叫从 R 到 R' 的一个同构对应或同构映射，或简称同构.

我们有

定理 8 设 R 和 R' 是两个同构的交换环，而

$$\sigma: R\to R'$$

是从 R 到 R' 的一个同构对应，那么有

i) R 的零元素 0 在 σ 之下的象 $0'=\sigma(0)$ 是 R' 的零元素.

ii) R 中任一元素 a 的负元素 $-a$ 在 σ 之下的象 $\sigma(-a)=-\sigma(a)$.

iii) 如果 R 有单位元素 e, e 在 σ 之下的象 $e'=\sigma(e)$ 就是 R' 的单位元素.

iv) 如果 R 没有零因子, R' 也没有零因子.

v) 如果 R 是域, R' 也一定是域.

证. i), ii), iii)的证明与§3定理4中相应的证明完全一样,我们就不重复了.

现在来证明 iv). 设 a', $b'\in R'$ 而 $a'b'=0'$. 因 σ 是从 R 到 R' 的一一对应,所以有 a, $b\in R$ 使

$$\sigma(a)=a',\ \sigma(b)=b'.$$

那么因 σ 是同构对应,

$$\sigma(ab)=\sigma(a)\sigma(b)=a'b'=0'.$$

仍因 σ 是一一对应,所以一定有

$$ab=0.$$

因 R 没有零因子,所以 $a=0$ 或 $b=0$. 于是

$$a'=\sigma(a)=\sigma(0)=0'$$

或

$$b'=\sigma(b)=\sigma(0)=0'.$$

因此 R' 也没有零因子.

再来证明 v). 设 R 是域,而 e 是它的单位元素. 那么根据 iii), $e'=\sigma(e)$就是 R' 的单位元素.对任意 $a'\in R'$ 而 $a'\neq 0'$, 因 σ 是一一对应, 就有 $a\in R$, $a\neq 0$ 而 $\sigma(a)=a'$. 因 R 是域, 所以有 $a^{-1}\in R$ 使 $aa^{-1}=e$. 因 σ 是同构对应, 所以有 $\sigma(a)\cdot\sigma(a^{-1})=\sigma(e)=e'$. 这就是说 $\sigma(a^{-1})$ 是 $\sigma(a)=a'$ 的逆元素.这证明了 R' 是域.

§7 商群和同余类环

设G是一个交换群，它的运算符号写作'+'，它的单位元素记作0，它里面任意一个元素a的逆元素记作$-a$. 再设H是G的一个子群，即H是G的一个非空子集而它对于G中运算'+'来说是一个群. 设a是G中任一元素，令

$$a+H=\{a+h \mid h\in H\}.$$

我们把$a+H$叫做H的一个陪集，而a叫做这个陪集的一个代表元. 特别$0+H$也是一个陪集，我们把它记作H. 我们有

引理1 设G是一个交换群，而H是它的一个子群，那么H的任意两个陪集或者没有公共元素，或者相等. 特别$h+H=H$，对任一$h\in H$.

证. 设$a+H$和$b+H$是H的两个陪集，而$a, b\in G$. 假定它们有一个公共元素c. 从$c\in a+H$可知$c=a+h_0$, $h_0\in H$. 于是对任意$h\in H$:

$$c+h=(a+h_0)+h=a+(h_0+h)\in a+H.$$

即$c+H\subset a+H$. 另一方面，$a=c+(-h_0)$. 于是对任意$h\in H$:

$$\begin{aligned}a+h&=(c+(-h_0))+h\\&=c+(-h_0+h)\in c+H.\end{aligned}$$

即$a+H\subset c+H$. 因此$a+H=c+H$. 同理可证$b+H=c+H$. 所以$a+H=b+H$. 这证明了H的两个陪集如果有一个公共元素，就一定相等. 换句话说，H的两个陪集或者没有公共元素，或者相等.

特别，对$h\in H$, $h=h+0\in h+H$, $h=0+h\in 0+H=H$. 因此$h+H=H$.

定理1 设G是一个交换群，而H是它的一个子群，那么

G 可唯一地表成 H 的一些两两没有公共元素的陪集的并. 设

$$G=\bigcup_{\alpha\in J}(a_\alpha+H)$$

是这样一个分解, 其中 J 是一个足码的集合, 那么记

$$G/H=\{a_\alpha+H\mid\alpha\in J\}.$$

对 H 的任意两个陪集 $a_\alpha+H$ 和 $a_\beta+H$, 定义

$$(a_\alpha+H)+(a_\beta+H)=(a_\alpha+a_\beta)+H, \tag{1}$$

那么这个定义不依赖于陪集的代表元的选择, 即如果 $a_\alpha+H=b_\alpha+H$, $a_\beta+H=b_\beta+H$, 那么

$$(a_\alpha+a_\beta)+H=(b_\alpha+b_\beta)+H.$$

因此可以把(1)看作是 G/H 中元素的运算, 而 G/H 对于按(1)式规定的运算是一个交换群.

证. G 的任一元素 a 一定属于 H 的一个陪集 $a+H$. 根据引理 1, H 的两个陪集或者没有公共元素或者相等, 因此, 如果在陪集集合

$$\{a+H\mid a\in G\}$$

里把重复的取消, 就得到 G 分解成 H 的一些两两没有公共元素的陪集的并的一个分解.

假定 $\quad G=\bigcup_{\alpha\in J_1}(a_\alpha+H),\quad G=\bigcup_{\beta\in J_2}(a_\beta+H)$

是 G 分成 H 的一些两两没有公共元素的陪集的并的两个分解, 其中 J_1 和 J_2 都是足码集合. 令

$$M_1=\{a_\alpha+H\mid\alpha\in J_1\},\quad M_2=\{a_\beta+H\mid\beta\in J_2\}.$$

对任意 $a_\alpha+H\in M_1$, 因 $a_\alpha\in G$, 所以一定有一个 $\beta\in J_2$ 使 $a_\alpha\in a_\beta+H$. 根据引理 1, $a_\alpha+H=a_\beta+H\in M_2$. 同理可证, 对任意 $a_\beta+H\in M_2$, 都有 $a_\beta+H\in M_1$. 因此 $M_1=M_2$. 这证明了将 G 表成 H 的一些两两没有公共元素的陪集的并的表法是唯一的.

设 $a_\alpha+H=b_\alpha+H$, $a_\beta+H=b_\beta+H$, 那么 $a_\alpha=b_\alpha+h_1$,

$a_\beta=b_\beta+h_2$, 而 $h_1,\ h_2\in H$. 于是

$$(a_\alpha+a_\beta)+H=(b_\alpha+h_1)+(b_\beta+h_2)+H$$
$$=(b_\alpha+b_\beta)+(h_1+h_2+H),$$

但根据引理 1 有 $h_1+h_2+H=H$. 因此

$$(a_\alpha+a_\beta)+H=(b_\alpha+b_\beta)+H,$$

即 $$(a_\alpha+H)+(a_\beta+H)=(b_\alpha+H)+(b_\beta+H).$$

这证明了(1)确实在 G/H 中规定了一个运算.

显然G/H对于(1)所规定的运算是自封的. 对任意$a_\alpha+H$, $a_\beta+H$, $a_\gamma+H\in G/H$, 根据(1)和 G 中交换律和结合律成立, 我们有

$$(a_\alpha+H)+(a_\beta+H)=(a_\alpha+a_\beta)+H$$
$$=(a_\beta+a_\alpha)+H=(a_\beta+H)+(a_\alpha+H),$$
$$((a_\alpha+H)+(a_\beta+H))+(a_\gamma+H)$$
$$=((a_\alpha+a_\beta)+H)+(a_\gamma+H)$$
$$=((a_\alpha+a_\beta)+a_\gamma)+H=(a_\alpha+(a_\beta+a_\gamma))+H$$
$$=(a_\alpha+H)+((a_\beta+a_\gamma)+H)$$
$$=(a_\alpha+H)+((a_\beta+H)+(a_\gamma+H)).$$

因此 G/H 中交换律和结合律也成立. 又 H 是 H 的一个陪集, 即 $H\in G/H$, 而

$$(a+H)+H=a+H \quad 对任意\ a+H\in G/H.$$

这就是说 H 是 G/H 的单位元素. 最后对任意 $a+H\in G/H$, $(-a)+H$ 也是 H 的一个陪集, 而

$$(a+H)+((-a)+H)$$
$$=(a+(-a))+H=0+H=H.$$

这就是说 $(-a)+H$ 是 $a+H$ 的逆元素, 因此 G/H 是一个交换群.

这样定理 1 就完全证明了.

定义 1 设 G 是一个交换群, 而 H 是 G 的一个子群, 我

们把 G/H 对于按(1)定义的运算所组成的交换群叫做交换群 G 对于子群 H 的商群，简称商群．

例 1 设 m 是个正整数，我们知道 $m\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个理想，因此 $m\mathbf{Z}$ 是 $\mathbf{Z}$ 的加法群的一个子群．容易看出商群 $\mathbf{Z}/m\mathbf{Z}$ 由下面这 m 个元素组成，它们是

$$0+\mathbf{Z}=\mathbf{Z},\ 1+\mathbf{Z},\ 2+\mathbf{Z},\ \cdots,\ (m-1)+\mathbf{Z}.$$

例 2 设 F 是一个域，$f(x)$ 是 $F[x]$ 中的一个 n 次多项式．我们知道 $(f(x))$ 是 $F[x]$ 的一个理想，因此 $(f(x))$ 是 $F[x]$ 的加法群的一个子群，于是我们有商群 $F[x]/(f(x))$．我们来证明，$(f(x))$ 的每一个陪集中都含有唯一的一个次数小于 $\partial^0 f(x)$ 的多项式．设 $g(x)+(f(x))$ 是任一陪集，根据带余除法，有

$$g(x)=q(x)f(x)+r(x),\quad \partial^0 r(x)<\partial^0 f(x),$$

那么 $\quad r(x)=g(x)+(-q(x))f(x)\in g(x)+(f(x)).$

设又有 $r_1(x)\in g(x)+(f(x))$ 而 $\partial^0 r_1(x)<\partial^0 f(x)$，那么

$$r_1(x)+(f(x))=g(x)+(f(x))=r(x)+(f(x)).$$

于是
$$r_1(x)=r(x)+k(x)f(x),$$
即
$$r_1(x)-r(x)=k(x)f(x).$$

因此 $f(x)\mid r_1(x)-r(x)$．但

$$\partial^0(r_1(x)-r(x))\leqslant \max(\partial^0 r(x),\quad \partial^0 r_1(x))<\partial^0 f(x).$$

因此 $r_1(x)=r(x)$．这证明了 $(f(x))$ 的每一个陪集中都含有唯一的一个次数小于 $\partial^0 f(x)$ 的多项式．我们可以选取这个次数小于 $\partial^0 f(x)$ 的多项式作为陪集的代表元．这样一来，

$$F[x]/(f(x))=\{a_0+a_1x+a_2x^2+\cdots \\ +a_{n-1}x^{n-1}+(f(x))\mid a_i\in F\}.$$

定义 2 设 G 是一个交换群，而 H 是 G 的一个子群，设 $a,b\in G$．如果 a 和 b 属于 H 的同一个陪集，即 $a+H=b+H$，也即 $a-b\in H$，那么就写

$$a \equiv b \pmod H,$$

读作 a 同余 b 模 H，并把它叫做模 H 的同余式，简称同余式.

特别，在例 1 中，我们把

$$a \equiv b \pmod{m\mathbf{Z}}$$

简记作
$$a \equiv b \pmod m$$

显然，$a \equiv b \pmod m$，当且仅当 $m \mid a-b$. 在例 2 中，我们把

$$g(x) \equiv h(x) \quad (\bmod (f(x)))$$

简记作
$$g(x) \equiv h(x) \quad (\bmod f(x)).$$

显然，$g(x) \equiv h(x) (\bmod f(x))$，当且仅当 $f(x) \mid g(x)-h(x)$.

定理 2 设 G 是一个交换群，而 H 是 G 的一个子群，再设 $a_\alpha, a_\beta, b_\alpha, b_\beta \in G$. 如果

$$a_\alpha \equiv b_\alpha \pmod H, \quad a_\beta \equiv b_\beta \pmod H,$$

那么
$$a_\alpha + a_\beta \equiv b_\alpha + b_\beta \pmod H.$$

证. 我们知道，$a_\alpha \equiv b_\alpha \pmod H$，当且仅当 $a_\alpha + H = b_\alpha + H$；$a_\beta \equiv b_\beta \pmod H$，当且仅当 $a_\beta + H = b_\beta + H$，而 $a_\alpha + a_\beta \equiv b_\alpha + b_\beta \pmod H$，当且仅当 $(a_\alpha + a_\beta) + H = (b_\alpha + b_\beta) + H$. 因此本定理只不过是定理 1 中所证明的 G/H 中元素的运算(1)的定义不依赖于陪集的代表元的选择这一结果的一个等价的说法而已.

引理 2 设 G 是个有限交换群，而 H 是它的一个子群，那么 H 的陪集中的元素个数都相等.

证. 因 G 是有限交换群，H 也是有限交换群，设 $a+H$ 是 H 的任一陪集. 显然从 H 到 $a+H$ 的映射

$$h \to a+h, \ h \in H,$$

是一对一的，而且是映上的，因此 H 和 $a+H$ 的元素个数相等.

定理 3 设 G 是个有限交换群，而 H 是它的一个子群，那么 $|G/H| = |G|/|H|$.

证. 设 $|G/H|=n$. 那么可以将 G 表成 H 的 n 个两两没有公共元素的陪集的并

$$G=\bigcup_{i=1}^{n}(a_i+H).$$

于是
$$|G|=\sum_{i=1}^{n}|a_i+H|=\sum_{i=1}^{n}|H|=n|H|.$$

因此
$$|G/H|=n=|G|/|H|.$$

现在设 R 是一个交换环, 而 I 是它的一个理想, 我们知道 I 是 R 的加法群的子群, 所以可以唯一地将 R 表成 I 的一些两两没有共同元素的陪集 $a_\alpha+I$ 的并

$$R=\bigcup_{\alpha\in J}(a_\alpha+I),$$

其中 J 是一个足码集合, 我们把 I 的陪集叫做 I 的同余类. 记

$$R/I=\{a_\alpha+I\,|\,\alpha\in J\}.$$

我们有

定理 4 设 R 是一个交换环, 而 I 是它的一个理想. 对于 R/I 中任意两个元素 $a_\alpha+I$ 和 $a_\beta+I$, 我们定义

$$(a_\alpha+I)+(a_\beta+I)=(a_\alpha+a_\beta)+I, \tag{2}$$

$$(a_\alpha+I)\cdot(a_\beta+I)=(a_\alpha a_\beta)+I, \tag{3}$$

那么这两个定义都不依赖于同余类的代表元的选择, 因而可以看作 R/I 中的加法运算和乘法运算, 更进一步, R/I 对于按(2), (3)所规定的加法运算和乘法运算是一个交换环.

证. R/I 中加法的定义(2)不依赖于同余类的代表元的选择已在定理 1 中证明, 现在来证 R/I 中乘法的定义 (3) 亦如此. 设 $a_\alpha+I=b_\alpha+I$, $a_\beta+I=b_\beta+I$, 那么 $a_\alpha=b_\alpha+h_1$, $a_\beta=b_\beta+h_2$, 而 h_1, $h_2\in I$. 于是

$$\begin{aligned}a_\alpha a_\beta+I&=(b_\alpha+h_1)(b_\beta+h_2)+I\\&=(b_\alpha b_\beta+b_\alpha h_2+b_\beta h_1+h_1h_2)+I,\end{aligned}$$

因 I 是 R 的理想, $b_\alpha h_2+h_\beta h_1+h_1h_2\in I$. 所以

$$a_\alpha a_\beta + I = (b_\alpha b_\beta + b_\alpha h_2 + b_\beta h_1 + h_1 h_2) + I = b_\alpha b_\beta + I.$$

这证明 R/I 中乘法的定义 (3) 也不依赖于陪集的代表元的选择.

显然 R/I 对于按(2), (3)规定的加法运算和乘法运算是自封的. 由定理1可知 R/I 对于加法运算来说是一个交换群. 还需要证明在 R/I 中 II.1, II.2 和 III 成立. 举II.1为例, 其余两个的证明方法一样. 设 $a_\alpha + I, a_\beta + I \in R/I$. 根据(3)和 R 中乘法交换律成立, 我们有

$$\begin{aligned}(a_\alpha + I)(a_\beta + I) &= a_\alpha a_\beta + I = a_\beta a_\alpha + I \\ &= (a_\beta + I)(a_\alpha + I).\end{aligned}$$

因此 II.1 在 R/I 中成立. 这证明了 R/I 是一个交换环.

定义 3 设 R 是一个交换环, 而 I 是 R 的一个理想. 我们把 R/I 按(2), (3)定义的加法运算和乘法运算所组成的交换环叫做交换环 R 对于理想 I 的同余类环, 也叫做 R 模 I 的同余类环, 简称同余类环.

定理 5 设 R 是一个交换环, 而 I 是 R 的一个理想, 再设 $a_\alpha, a_\beta, b_\alpha, b_\beta \in R$. 如果

$$a_\alpha \equiv b_\alpha (\bmod I), \quad a_\beta \equiv b_\beta (\bmod I)$$

那么

$$a_\alpha a_\beta \equiv b_\alpha b_\beta (\bmod I).$$

证. 本定理只是定理4中所证明的 R/I 中元素的运算(3)的定义不依赖于同余类的代表元的选择这一结果的一个等价的叙述.

我们再回去讨论例1和例2.

例 1(续) 根据定理4, 我们知道 $\mathbf{Z}/m\mathbf{Z}$ 是个交换环, 叫做整数环 $\mathbf{Z}$ 模 m 的同余类环. 这个交换环实质上就是以前讨论的交换环 $\mathbf{Z}_m$. 我们有

定理 6 设 m 是任一正整数, 那么从 $\mathbf{Z}_m$ 到 $\mathbf{Z}/m\mathbf{Z}$ 的一一对应

$$k \to k+(m), \quad 0 \leqslant k \leqslant m-1$$

是个同构对应.

证. 这是因为

$$k+l \equiv (k+l)_m \quad (\bmod m),$$
$$kl \equiv (kl)_m \qquad (\bmod m).$$

从这个定理可以知道,我们为什么要在 $\mathbf{Z}_m$ 中如下地规定加法和乘法:

$$k \oplus l = (k+l)_m$$
$$k \odot l = (kl)_m.$$

系理 设 p 是任一素数,那么 $\mathbf{Z}/p\mathbf{Z}$ 是 p 个元素的域.

证. 这是定理 6 和 § 6 定理 8 的推论.

例 2(续) 根据定理 4, 我们知道 $F[x]/(f(x))$ 是个交换环,叫做域 F 上一个文字 x 的多项式环 $F[x]$ 模 $f(x)$ 的同余类环. 平行于定理 6 及其系理,我们有

定理 7 设 F 是一个域, $f(x)$ 是 $F[x]$ 中的一个 $\neq 0$ 的多项式,那么从 $F[x]_{f(x)}$ 到 $F[x]/(f(x))$ 的一一对应

$$g(x) \to g(x)+(f(x)), \ \partial^0 g(x) < \partial^0 f(x)$$

是个同构对应.

系理 设 F 是一个域,而 $p(x)$ 是 $F[x]$ 中的一个不可约多项式,那么 $F[x]/(p(x))$ 是域.

由于它们的证明与定理 6 及其系理的证明完全一样, 我们就不重复了.

§ 8 孙子定理和环的直和分解

设 m 是一个大于 1 的整数,并假定

$$m = m_1 m_2 \cdots m_r,$$

其中 $m_1, m_2, \cdots, m_r$ 是 r 个两两互素的大于 1 的整数. 对任

一 $n\in \mathbf{Z}_m$，我们有

$$(n)_{m_i}\in \mathbf{Z}_{m_i}, \quad 对\ i=1, 2, \cdots, r.$$

问题是，反过来，任给 $n_i\in \mathbf{Z}_{m_i}$，$i=1, 2, \cdots, r$，是否有 $n\in \mathbf{Z}_m$ 使

$$(n)_{m_i}=n_i, 对\ i=1, 2, \cdots, r.$$

即是否有 $n\in \mathbf{Z}_m$ 使同余式

$$n\equiv n_i(\mathrm{mod}\, m_i),\ i=1, 2, \cdots, r,$$

同时成立．这个问题的答案是肯定的，这就是

定理 1（孙子定理） 设 $m_1, m_2, \cdots, m_r$ 是 r 个两两互素的大于 1 的整数，令

$$m=m_1m_2\cdots m_r,$$

那么任给 $n_i\in \mathbf{Z}_{m_i}$，$i=1, 2, \cdots, r$，有唯一的一个 $n\in \mathbf{Z}_m$ 使下面这 r 个同余式

$$n\equiv n_i(\mathrm{mod}\, m_i), \quad i=1, 2, \cdots, r \tag{1}$$

同时成立．

证．令

$$\widehat{m}_i=\frac{m}{m_i}, \quad i=1, 2, \cdots, r.$$

那么 $\widehat{m}_1, \widehat{m}_2, \cdots, \widehat{m}_r$ 的最大公因数是 1．根据 §6 定理 5 的系理，有 r 个整数 $c_1, c_2, \cdots, c_r$ 存在使

$$1=c_1\widehat{m}_1+c_2\widehat{m}_2+\cdots+c_r\widehat{m}_r. \tag{2}$$

显然有 $$c_i\widehat{m}_i\equiv 1(\mathrm{mod}\, m_i), \quad i=1, 2, \cdots, r,$$

$$c_i\widehat{m}_i\equiv 0(\mathrm{mod}\, m_j) \quad 对\ j\neq i.$$

如果令 $$n=(c_1\widehat{m}_1n_1+c_2\widehat{m}_2n_2+\cdots+c_r\widehat{m}_rn_r)_m,$$

那么 $n\in \mathbf{Z}_m$ 而

$$n\equiv n_i(\mathrm{mod}\, m_i), \quad i=1, 2, \cdots, r.$$

更进一步，假设还有 $n'\in \mathbf{Z}_m$ 而 n' 适合

$$n'\equiv n_i(\mathrm{mod}\, m_i), \quad i=1, 2, \cdots, r.$$

设 $n\geqslant n'$，那么

$$n-n'\equiv 0 \pmod{m_i}, \quad i=1, 2, \cdots, r.$$

这就是说 $\quad m_i \mid n-n', \quad i=1, 2, \cdots, r.$

因 $m_1, m_2, \cdots, m_r$ 两两互素，所以

$$m \mid n-n'.$$

但 $n, n' \in \mathbf{Z}_m$，而 $n \geqslant n'$，所以 $0 \leqslant n-n' < m$. 因此一定有 $n-n'=0$，即 $n=n'$. 这证明了 $\mathbf{Z}_m$ 中适合同余式组(1)的元素 n 是唯一确定的.

例 "今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？"（见孙子算经，"物不知其数"一问题）

这个问题是要求一个正整数 n 适合下面三个同余式

$$n \equiv 2 \pmod{3},$$
$$n \equiv 3 \pmod{5},$$
$$n \equiv 2 \pmod{7}.$$

孙子算经中给出了解这个问题的一个算法.

"术曰：三三数之剩二，置一百四十，五五数之剩三，置六十三；七七数之剩二，置三十；并之得二百三十三；以二百一十减之即得. 凡三三数之剩一，则置七十；五五数之剩一，则置二十一；七七数之剩一，则置十五；一百六以上，以一百五减之即得."

孙子算经(3—5世纪).

后来，程大位将这一算法编成一个歌诀：

"三人同行七十稀，
五树梅花廿一枝，
七子团圆正半月，
除百零五便得知."

程大位，算法统宗(1593).

这个歌诀的意思是说：用 70 去乘用 3 去除 n 所得的余数 2，用 21 去乘用 5 去除 n 所得的余数 3，再用 15 去乘用 7 去除 n

所得的余数 2，将所得的三个数 70×2，21×3，15×2 相加．然后再将所得的和 $70\times2+21\times3+15\times2$ 用 105 去除，所得的余数就是 n． 即

$$n=(70\times2+21\times3+15\times2)_{105}=23.$$

我们知道 $105=3\times5\times7$，但 70，21，15 这三个数怎样来的呢？

显然 $5\times7=35$，$3\times7=21$，$3\times5=15$ 这三个数的最大公因数是 1，因此有三个整数 c_1，c_2，c_3 使

$$c_1\cdot35+c_2\cdot21+c_3\cdot15=1. \tag{3}$$

令 $$e_1=c_1\cdot35,\quad e_2=c_2\cdot21,\quad e_3=c_3\cdot15,$$

那么由(3)式可得

$$\left.\begin{array}{lll} e_1\equiv1(\bmod 3), & e_1\equiv0(\bmod 5), & e_1\equiv0(\bmod 7), \\ e_2\equiv0(\bmod 3), & e_2\equiv1(\bmod 5), & e_2\equiv0(\bmod 7), \\ e_3\equiv0(\bmod 3), & e_3\equiv0(\bmod 5), & e_3\equiv1(\bmod 7). \end{array}\right\} \tag{4}$$

于是 $$n=(e_1\cdot2+e_2\cdot3+e_3\cdot2)_{105}.$$

当然可以用辗转相除法求出适合(3)式的 c_1，c_2，c_3，再由 c_1，c_2，c_3 算出 e_1，e_2，e_3． 但也可以直接求适合条件(4)的 e_1，e_2，e_3．从(4)中第一行的三个同余式可知，e_1 需要是 5 和 7 的倍数中被 3 除余 1 的一个，而 70 就是这样的一个数．从(4)中第二行的三个合余式可知，e_2 需要是 3 和 7 的倍数中被 5 除余 1 的一个，而 21 就是这样的一个数． 从(4)中第三行的三个同余式可知，e_3 需要是 3 和 5 的倍数中被 7 除余 1 的一个，而 15 就是这样的一个数．这说明 70，21，15 这三个数的由来．

基于上面例题的解法，我们可以给定理 1 的证明加一注记，当然在定理 1 的证明中，可以用辗转相除法求出 c_1，c_2，…，c_n 使

$$c_1\widehat{m}_1+c_2\widehat{m}_2+\cdots+c_n\widehat{m}_n=1,$$

再令 $e_i=(c_i\widehat{m}_i)_m \quad i=1, 2, \cdots, r,$

就求出了 $e_1, e_2, \cdots, e_n$. 但也可以直接求解它们所适合的同余式组:

$$\left.\begin{aligned} &e_i\equiv1(\operatorname{mod} m_i), \\ &e_i\equiv0(\operatorname{mod} m_j), \quad 如\ j\neq i, \end{aligned}\right\} i, j=1, 2, , \cdots, r.$$

因 m_i 和 $\widehat{m}_i$ 互素，故用辗转相除法可求得 a_i 和 b_i 使

$$a_i\widehat{m}_i+b_im_i=1, \quad i=1, 2, \cdots, r.$$

那么取 $e_i=(a_i\widehat{m}_i)_m, \quad i=1, 2, \cdots, r$

即可.

因此我们可以给出定理 1 中 n 的存在性的另一证明:

证. 令 $\widehat{m}_i=\dfrac{m}{m_i}, \quad i=1, 2, \cdots, r,$

那么 $\widehat{m}_i$ 和 m_i 互素 $(i=1, 2, \cdots, r)$. 于是有整数 a_i 和 $b_i(i=1, 2, \cdots, r)$ 存在使

$$a_i\widehat{m}_i+b_im_i=1, \quad i=1, 2, \cdots, r.$$

令 $$e_i=(a_i\widehat{m}_i)_m,$$

那么 $e_i\in\mathbf{Z}_m$ 而

$$\left.\begin{aligned} &e_i\equiv1(\operatorname{mod} m_i), \\ &e_i\equiv0(\operatorname{mod} m_j), 如果\ j\neq i, \end{aligned}\right\} i, j=1, 2, \cdots, r. \tag{5}$$

因此，如果令 $n=(e_1n_1+e_2n_2+\cdots+e_rn_r)_m,$

则 $n\in\mathbf{Z}_m$ 而 $n\equiv n_i(\operatorname{mod} m_i), \quad i=1, 2, \cdots, r.$

系理 1 设 $m_1, m_2, \cdots, m_r$ 是 r 个两两互素的大于 1 的整数，令

$$m=m_1m_2\cdots m_r,$$

那么对任意 $n\in\mathbf{Z}_m^*$, 我们有 $(n)_{m_i}\in\mathbf{Z}_{m_i}^*$. 反过来，任给 $n_i\in\mathbf{Z}_{m_i}^*$, $i=1, 2, \cdots, r$, 那么有唯一的一个 $n\in\mathbf{Z}_m^*$ 使 (1) 中 r 个同余式同时成立.

证. 设 $n\in\mathbf{Z}_m^*$, 那么 $(n, m)=1$. 于是 $(n, m_i)=1$. 因此

$((n)_{m_i},\ m_i)=1$, 即 $(n)_{m_i}\in\mathbf{Z}^*_{m_i}$.

反之，任给 $n_i\in\mathbf{Z}^*_{m_i}$, $i=1, 2, \cdots, r$. 根据孙子定理，有唯一的一个 $n\in\mathbf{Z}_m$ 使下面 r 个同余式

$$n\equiv n_i(\mathrm{mod}\ m_i),\quad i=1, 2, \cdots, r$$

同时成立. 因 $n_i\in\mathbf{Z}^*_{m_i}$, 所以 $(n_i, m_i)=1$. 那么由上式推出 $(n, m_i)=1$, $i=1, 2, \cdots, r$. 因 $m=m_1m_2\cdots m_r$ 而 $m_1, m_2, \cdots, m_r$ 两两互素，所以 $(n, m)=1$, 即 $n\in\mathbf{Z}^*_m$.

系理 2 设 $m_1, m_2, \cdots, m_r$ 是 r 个两两互素的大于 1 的整数. 令

$$m=m_1m_2\cdots m_r,$$

那么
$$\varphi(m)=\varphi(m_1)\varphi(m_2)\cdots\varphi(m_r),$$

这里 $\varphi(m)$ 是群 $\mathbf{Z}^*_m$ 的阶，即小于m的正整数中与m互素的个数. 特别，如果

$$m=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r},$$

其中 $p_1, p_2, \cdots, p_r$ 是 r 个两两不同的素数，而 $e_1, e_2, \cdots, e_r$ 都是 $\geqslant 1$ 的整数，那么

$$\varphi(m)=\prod_{i=1}^{r} p_i^{e_i-1}(p_i-1)=m\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

证. 系理 1 的第一部分是说，任给 $n\in\mathbf{Z}^*_m$ 都对应着 $\mathbf{Z}^*_{m_1}$ 中的一个元素 $(n)_{m_1}$, $\mathbf{Z}^*_{m_2}$ 中的一个元素 $(n)_{m_2}$, $\cdots$, $\mathbf{Z}^*_{m_r}$ 中的一个元素 $(n)_{m_r}$. 而系理 1 的第二部分是说，这个对应是映上的而且是一一的. 因此

$$|\mathbf{Z}^*_m|=|\mathbf{Z}^*_{m_1}|\cdot|\mathbf{Z}^*_{m_2}|\cdot\cdots\cdot|\mathbf{Z}^*_{m_r}|,$$

即
$$\varphi(m)=\varphi(m_1)\varphi(m_2)\cdots\varphi(m_r).$$

特别，如果

$$m=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r},$$

其中 $p_1, p_2, \cdots, p_r$ 是两两不同的素数，而 $e_1, e_2, \cdots, e_r$ 都是 $\geqslant 1$ 的整数，那么

$$\varphi(m)=\varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_r^{e_r}).$$

在小于 $p_i^{e_i}$ 的非负整数中，只有下面这 $p_i^{e_i-1}$ 个数

$$0,\ p_i,\ 2p_i,\ \cdots,\ (p_i^{e_i-1}-1)p_i$$

不与 p_i 互素．因此

$$\varphi(p_i^{e_i})=p_i^{e_i}-p_i^{e_i-1}=p_i^{e_i-1}(p_i-1).$$

所以
$$\varphi(m)=\prod_{i=1}^{r}p_i^{e_i-1}(p_i-1)=m\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

这就是在§4中所留待证明的公式．

孙子定理是我国古代数学的重要成就之一，过去在国外的一些数学文献里往往被叫做中国剩余定理，它是近代抽象代数中环的直和分解这一概念的重要源泉，而它的证明中的(2)式，特别是在 $\mathbf{Z}_m$ 中求一组适合同余式组(5)的 $e_1,\ e_2,\ \cdots,\ e_r$ 则是近代环论中寻求环的一组两两正交的幂等元并使得环的单位元素可以表成它们的和这一基本工具的重要源泉．

定理 2 设 $m_1,\ m_2,\ \cdots,\ m_r$ 是 r 个两两互素的大于1的整数．令

$$m=m_1m_2\cdots m_r,$$

并令
$$\widehat{m}_i=\frac{m}{m_i},\quad i=1,\ 2,\ \cdots r,$$

那么对任一 $i=1,\ 2,\ \cdots,\ r$，$\widehat{m}_i$ 和 m_i 的最大公因数都是1，因而有一对整数 a_i 和 b_i 存在使

$$a_i\widehat{m}_i+b_im_i=1,\quad i=1,\ 2,\ \cdots,\ r. \tag{6}$$

再令
$$e_i=(a_i\widehat{m}_i)_m,\qquad i=1,\ 2,\ \cdots,\ r.$$

仍把 $\mathbf{Z}_m$ 中的加法运算符号和乘法运算符号分别记作$\oplus$和$\odot$，那么

i) $e_1,\ e_2,\ \cdots,\ e_r$ 都是 $\mathbf{Z}_m$ 中不等于0的元素，而且

$$e_i^2=e_i\odot e_i=e_i,\quad i=1,\ 2,\ \cdots,\ r.$$

$$e_i\odot e_j=0,\qquad \text{如果 } i\neq j.$$

$$1=e_1\oplus e_2\oplus\cdots\oplus e_r.$$

ii) 令

$$\mathbf{Z}'_{m_i}=e_i\mathbf{Z}_m=\{e_i\odot n\mid n\in\mathbf{Z}_m\},\quad i=1,2,\cdots,r,$$

那么 $\mathbf{Z}'_{m_i}$ 是 $\mathbf{Z}_m$ 的理想，e_i 是它的单位元素，而映射

$$\sigma_i: k\to e_i\odot k,\quad 0\leqslant k<m_i$$

是从 $\mathbf{Z}_{m_i}$ 到 $\mathbf{Z}'_{m_i}$ 之上的同构对应.

iii) $\mathbf{Z}_m$ 中任一元素 n 都可以唯一地表成 $\mathbf{Z}'_{m_1}$ 中一个元素，$\mathbf{Z}'_{m_2}$ 中一个元素，… 和 $\mathbf{Z}'_{m_r}$ 中一个元素的和．实际上，

$$n=e_1\odot n\oplus e_2\odot n\oplus\cdots\oplus e_r\odot n.$$

证，先证 i)．显然有

$$\left.\begin{aligned}&e_i\equiv1(\operatorname{mod} m_i),\\&e_i\equiv0(\operatorname{mod} m_j),\quad\text{如果 } j\neq i,\end{aligned}\right\}i,\ j=1,2,\cdots,r.\tag{7}$$

因此 $e_i\neq0(i=1,2,\cdots,r)$．再根据 §7 定理 4 就有

$$e_i^2\equiv1(\operatorname{mod} m_i),$$
$$e_i^2\equiv0(\operatorname{mod} m_j),\quad\text{如果 } j\neq i.$$

于是根据孙子定理的唯一性部分就推出

$$(e_i^2)_m=e_i,\quad i=1,2,\cdots,r.$$

这就是说 $\qquad e_i\odot e_i=e_i,\quad i=1,2,\cdots,r.$

当 $i\neq j$ 时，根据 §7 定理 4，从(7)式推出

$$e_ie_j\equiv0(\operatorname{mod} m_k),\ k=1,2,\cdots,r.$$

仍根据孙子定理的唯一性部分有

$$(e_ie_j)_m=0,\quad\text{如果 } i\neq j.$$

这就是说 $\qquad e_i\odot e_j=0,\quad$ 如果 $i\neq j.$

又显然有

$$e_1+e_2+\cdots+e_r\equiv1(\operatorname{mod} m_i),\quad i=1,2,\cdots,r.$$

仍根据孙子定理的唯一性部分有

$$(e_1+e_2+\cdots+e_r)_m=1.$$

这就是说 $\qquad 1=e_1\oplus e_2\oplus\cdots\oplus e_r.\qquad(8)$

这证明了 i).

再证明 ii). 显然 $\mathbf{Z}'_{m_i}$ 是 $\mathbf{Z}_m$ 的由 e_i 生成的理想，$\mathbf{Z}'_{m_i}$ 中任一元素可表成 $e_i \odot n$, $n \in \mathbf{Z}_m$. 因此

$$e_i \odot (e_i \odot n) = (e_i \odot e_i) \odot n = e_i \odot n.$$

这就是说 e_i 是 $\mathbf{Z}'_{m_i}$ 的单位元素.我们再证明 σ_i 是同构对应.假定

$$e_i \odot k = e_i \odot l, \quad 0 \leqslant k, \ l < m_i,$$

那么
$$(a_i \hat{m}_i k)_m = (a_i \hat{m}_i l)_m,$$
于是
$$m \mid a_i \hat{m}_i (k-l),$$
因此
$$m_i \mid a_i (k-l).$$
但由(6)式知
$$(a_i, \ m_i) = 1,$$
所以
$$m_i \mid k-l.$$
又因 $0 \leqslant k, \ l < m_i$, 故有 $k = l$. 这证明 σ_i 是一对一的. 再证 σ_i 是映上的. 设 $e_i \odot n$ 是 $\mathbf{Z}'_{m_i}$ 中任一元素，其中 $n \in \mathbf{Z}_m$. 根据带余除法,

$$n = q m_i + r, \quad 0 \leqslant r < m_i,$$

那么因 $m = m_i \hat{m}_i$, 所以

$$\begin{aligned} e_i \odot n &= (a_i \hat{m}_i n)_m = (a_i \hat{m}_i (q m_i + r))_m \\ &= (a_i \hat{m}_i r)_m = e_i \odot r \end{aligned}$$

这证明了 $e_i \odot n$ 是 $r \in \mathbf{Z}_{m_i}$ 在 σ_i 之下的象，因此 σ_i 是个一一对应.

将 $\mathbf{Z}_{m_i}$ 中的加法运算符号和乘法运算符号分别记成 $\oplus_i$ 和 $\odot_i$. 因

$$e_i \odot m_i = (a_i \hat{m}_i m_i)_m = 0,$$

所以对任意 $k, \ l \in \mathbf{Z}_{m_i}$, 有

$$\begin{aligned} \sigma_i(k \oplus_i l) &= e_i \odot (k \oplus_i l) = e_i \odot (k+l)_{m_i} = e_i \odot (k+l)_m \\ &= (a_i \hat{m}_i (k+l))_m = (a_i \hat{m}_i k + a_i \hat{m}_i l)_m \\ &= (a_i \hat{m}_i k)_m \oplus (a_i \hat{m}_i l)_m = e_i \odot k \oplus e_i \odot l \\ &= \sigma_i(k) \oplus \sigma_i(l), \end{aligned}$$

$$
\begin{aligned}
\sigma_i(k\odot_i l) &= e_i\odot(k\odot_i l)=e_i\odot(kl)_{m_i} \\
&= e_i\odot(kl)_m=e_i\odot e_i\odot(kl)_m \\
&= (a_i\hat{m}_i\cdot a_i\hat{m}_i\cdot kl)_m=((a_i\hat{m}_i k)(a_i\hat{m}_i l))_m \\
&= (a_i\hat{m}_i k)_m\odot(a_i\hat{m}_i l)_m=(e_i\odot k)\odot(e_i\odot l) \\
&= \sigma_i(k)\odot\sigma_i(l).
\end{aligned}
$$

这证明了 σ_i 是个同构对应.

最后来证明 iii). 对任一 $n\in\mathbf{Z}_m$, 将 n 乘(8)式双方,得

$$
n=e_1\odot n\oplus e_2\odot n\oplus\cdots\oplus e_r\odot n,\quad e_i\odot n\in\mathbf{Z}_{m_i}.
$$

如果 n 还有另一种表法:

$$
n=e_1\odot n_1\oplus e_2\odot n_2\oplus\cdots\oplus e_r\odot n_r,\quad n_i\in\mathbf{Z}_{m_i}.
$$

将上式双方都乘以 e_i 得到

$$
e_i\odot n=e_i\odot n_i,
$$

即
$$
(a_i\hat{m}_i n)_m=(a_i\hat{m}_i n_i)_m.
$$

于是
$$
m\mid a_i\hat{m}_i(n-n_i),
$$

由此推出
$$
m_i\mid a_i(n-n_i).
$$

但$(m_i,\ a_i)=1$,所以

$$
m_i\mid n-n_i,
$$

因此
$$
e_i\odot n=e_i\odot n_i.
$$

上式对 $i=1,\ 2,\ \cdots,\ r$ 都成立,这证明了表法的唯一性.

这样定理 2 就完全证明了.

我们给出下面两个定义.

定义 1 设 R 是一个交换环, ε 是 R 的一个元素. 如果 $\varepsilon^2=\varepsilon$, ε 就叫做 R 的一个*幂等元*. 显然 R 的零元素 0 是幂等元. R 中除开 0 以外的幂等元叫做*非零幂等元*. 再设 e_1 和 e_2 是 R 的两个非零幂等元,如果 $e_1e_2=0$, 我们就说 e_1 和 e_2 *正交*.

定义 2 设 R 是一个交换环, 而 $R_1,\ R_2,\ \cdots,\ R_r$ 是 R 的 r 个理想. 如果 R 的每一个元素 a 都可以唯一地表成

$$a=a_1+a_2+\cdots+a_r,\quad a_i\in R_i,$$

我们就说 R 分成了它的理想 $R_1, R_2, \cdots, R_r$ 的直和，并记

$$R=R_1\dot{+}R_2\dot{+}\cdots\dot{+}R_r.$$

基于这两个定义，定理 2 的 i) 和 iii) 可以重新叙述成：

i) $e_1, e_2, \cdots, e_m$ 是 $\mathbf{Z}_m$ 的 r 个两两正交的非零幂等元，而 $\mathbf{Z}_m$ 的单位元素 1 分解成它们的和，

$$1=e_1\oplus e_2\oplus\cdots\oplus e_r.$$

iii) $\mathbf{Z}_m$ 分解成了它的理想 $\mathbf{Z}'_{m_1}, \mathbf{Z}'_{m_2}, \cdots, \mathbf{Z}'_{m_r}$ 的直和，即

$$\mathbf{Z}_m=\mathbf{Z}'_{m_1}\dot{\oplus}\mathbf{Z}'_{m_2}\dot{\oplus}\cdots\dot{\oplus}\mathbf{Z}'_{m_r}.$$

设 F 是域，$F[x]$ 是 F 上一个文字 x 的多项式环．那么对于 $F[x]$，有下面这一系列平行的结果．

定理 3(孙子定理) 设 F 是任意一域，$f_1(x), f_2(x), \cdots, f_r(x)$ 是 $F[x]$ 中 r 个两两互素的次数 $\geqslant 1$ 的多项式．令

$$f(x)=f_1(x)f_2(x)\cdots f_r(x),$$

那么对任一 $g(x)\in F[x]_{f(x)}$，都有 $(g(x))_{f_i(x)}\in F[x]_{f_i(x)}$，而

$$g(x)\equiv(g(x))_{f_i(x)}(\bmod f_i(x)).$$

反之，任给 $g_i(x)\in F[x]_{f_i(x)}$，$i=1, 2, \cdots, r$，都有唯一的一个 $g(x)\in F[x]_{f(x)}$ 使下面这 r 个同余式

$$g(x)\equiv g_i(x)(\bmod f_i(x)),\quad i=1, 2, \cdots, r,$$

同时成立．

系理 1 在定理 3 的前提下，对任一 $g(x)\in F[x]^*_{f(x)}$，都有 $(g(x))_{f_i(x)}\in F[x]^*_{f_i(x)}$．反之，任给 $g_i(x)\in F[x]^*_{f_i(x)}$，$i=1, 2, \cdots, r$，那么有唯一的一个 $g(x)\in F[x]^*_{f(x)}$ 使定理 3 中 r 个同余式同时成立．

设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个次数 $\geqslant 1$ 的多项式．用 $\Phi(f)$ 表示群 $\mathbf{F}_q[x]^*_{f(x)}$ 的阶．那么我们还有

系理 2 设 $f_1(x), f_2(x), \cdots, f_r(x)$ 是 $\mathbf{F}_q[x]$ 中 r 个两两互素的次数 $\geqslant 1$ 的多项式．令

$$f(x)=f_1(x)f_2(x)\cdots f_r(x),$$

那么
$$\Phi(f)=\Phi(f_1)\Phi(f_2)\cdots\Phi(f_r).$$

特别，如果每个 $f_i(x)$ 都是一个不可约多项式 $p_i(x)$ 的幂，譬如说 $f_i(x)=p_i(x)^{e_i}$，而 $\partial^0 p_i(x)=n_i(1\leqslant i\leqslant r)$，那么

$$\Phi(f)=\prod_{i=1}^{r}q^{n_i(e_i-1)}(q^{n_i}-1)=q^n\prod_{i=1}^{r}\left(1-\frac{1}{q^{n_i}}\right),$$

其中 $n=\sum_{i=1}^{r}n_ie_i$ 是 $f(x)$ 的次数.

定理 4 在定理 3 的前提下，令

$$\hat{f}_i(x)=f(x)/f_i(x),$$

那么对任一 $i=1, 2, \cdots, r$，$\hat{f}_i(x)$ 和 $f_i(x)$ 都互素，因而有 r 对多项式 $a_i(x)$ 和 $b_i(x)(i=1, 2, \cdots, r)$ 存在使

$$1=a_i(x)\hat{f}_i(x)+b_i(x)f_i(x),\quad i=1, 2, \cdots, r.$$

再令
$$e_i=(a_i(x)\hat{f}_i(x))_{f(x)},\quad i=1, 2, \cdots, r.$$

仍把 $F[x]_{f(x)}$ 中的加法运算符号和乘法运算符号分别记作 $\oplus$ 作 $\odot$，那么

i) $e_1, e_2, \cdots, e_r$ 是 $F[x]_{f(x)}$ 中 r 个两两正交的非零幂等元，即

$$e_i^2=e_i\odot e_i=e_i,\quad i=1, 2, \cdots, r,$$
$$e_i\odot e_j=0,\qquad 如果\ i\neq j.$$

而且
$$1=e_1\oplus e_2\oplus\cdots\oplus e_r.$$

ii) 令

$$F[x]'_{f_i(x)}=\{e_i\odot g(x)\mid g(x)\in F[x]_{f(x)}\},\ i=1, 2, \cdots, r,$$

那么 $F[x]'_{f_i(x)}$ 是 $F[x]_{f(x)}$ 的理想，e_i 是它的单位元素，而映射

$$\sigma_i: k(x)\to e_i\odot k(x),\quad k(x)\in F[x]_{f_i(x)}$$

是从 $F[x]_{f_i(x)}$ 到 $F[x]'_{f_i(x)}$ 之上的同构.

iii) $F[x]_{f(x)}$ 分解成它的理想 $F[x]'_{f_1(x)}$，$F[x]'_{f_2(x)}$，$\cdots$，

$F[x]'_{f_r(x)}$ 的直和

$$F[x]_{f(x)}=F[x]'_{f_1(x)}\dot{\oplus}F[x]'_{f_2(x)}\dot{\oplus}\cdots\dot{\oplus}F[x]'_{f_r(x)}.$$

由于这些定理的证明和前面相应的 $\mathbf{Z}$ 中的定理的证明完全一样，我们就不重复了.

关于一般的有单位元素的交换环的直和分解，我们有

定理 5 设 R 是有单位元素 1 的交换环，并假定 R 分解成 r 个非零理想 $R_1, R_2, \cdots, R_r$ 的直和

$$R=R_1\dot{+}R_2\dot{+}\cdots\dot{+}R_r. \tag{9}$$

设 1 在 R 的这个直和分解中表成

$$1=e_1+e_2+\cdots+e_r, \quad e_i\in R_i, \tag{10}$$

那么 $e_1, e_2, \cdots, e_r$ 是 r 个两两正交的非零幂等元，而且 e_i 是 R_i 的单位元素. 反过来，如果 1 分解成 r 个两两正交的非零幂等元的和(10)，令 $R_i=e_iR$，那么 R_i 是 R 的非零理想，而 R 是 $R_1, R_2, \cdots, R_r$ 的直和.

证. 先设 R 分解成它的 r 个非零理想 $R_1, R_2, \cdots, R_r$ 的直和(9)，而 R 的单位元素 1 在这个直和分解中分解成 $e_1, e_2, \cdots, e_r$ 的和，$e_i\in R_i$，即(10)式成立. 将(10)式双方乘以 e_i，得

$$e_i=e_ie_1+e_ie_2+\cdots+e_ie_i+\cdots+e_ie_r. \tag{11}$$

因 R_j 是 R 的理想，而 $e_j\in R_j$，所以 $e_ie_j\in R_j(j=1, 2, \cdots, r)$. 因此(11)就是 e_i 按 R 的直和分解(9)表成 R_1 的元素 e_ie_1，R_2 的元素 e_ie_2，$\cdots$，和 R_r 的元素 e_ie_r 的和的分解. 但 e_i 在直和分解(9)中显然可表成

$$e_i=0+0+\cdots+0+\underset{\text{第}\,i\,\text{项}}{e_i}+0+\cdots+0.$$

根据表示法的唯一性，推出

$$e_i\cdot e_i=e_i,$$

$$e_i\cdot e_j=0, \quad \text{如果 } i\neq j.$$

这证明了 $e_1, e_2, \cdots, e_r$ 是两两正交的幂等元. 更进一步, 设 a_i 是 R_i 中任一元素. 将(10)式双方乘以 a_i, 得

$$a_i = e_1 a_i + e_2 a_i + \cdots + e_i a_i + \cdots + e_r a_i.$$

仍因 R_j 是 R 的理想, 而 $e_j \in R_j$, 所以 $e_j a_i \in R_j (j=1, 2, \cdots, r)$. 因此上式就是 a_i 按 R 的直和分解(9)的表示, 但 a_i 显然又可表成

$$a_i = 0 + 0 + \cdots + 0 + \underset{\substack{第\\i\\项}}{a_i} + 0 + \cdots + 0.$$

仍根据表示法的唯一性, 推出

$$e_i a_i = a_i, \quad 对任意\ a_i \in R_i.$$

这证明了 e_i 是 R_i 的单位元素. 因 $R_i \neq (0)$, 所以 $e_i \neq 0$ ($i = 1, 2, \cdots, r$).

反过来, 设

$$1 = e_1 + e_2 + \cdots + e_r, \tag{10}$$

而 $e_1, e_2, \cdots, e_r$ 是 r 个两两正交的非零幂等元. 令

$$R_i = e_i R,$$

那么 R_i 是 R 中由 e_i 生成的理想, 而 e_i 是它的单位元素. 显然 $R_i \neq (0)$. 设 a 是 R 中任一元素, 将(10)式双方同时乘以 a, 得

$$a = e_1 a + e_2 a + \cdots + e_r a, \quad e_i a \in R_i.$$

设 a 有另一种方法表成 R_1 的一个元素 a_1, R_2 的一个元素 a_2, $\cdots$ 和 R_r 的一个元素 a_r 的和

$$a = a_1 + a_2 + \cdots + a_r, \quad a_i \in R_i.$$

将上式双方乘以 e_i, 得

$$e_i a = e_i a_1 + e_i a_2 + \cdots + e_i a_r.$$

因 e_j 是 R_j 的单位元素, 所以

$$e_i a_j = e_i (e_j a_j) = (e_i e_j) a_j = 0, \quad 如果\ i \neq j.$$

因此 $$e_ia=e_ia_i=a_i.$$
这证明了 a 可唯一地表成 R_1 的一个元素，R_2 的一个元素，$\cdots$ 和 R_r 的一个元素的和，这就是说 R 是 $R_1, R_2, \cdots, R_r$ 的直和.

定理 5 就完全证明了.

定义 3 设 R 是一个交换环，e 是 R 的一个非零幂等元. 如果 e 不能分解成两个互相正交的非零幂等元的和，e 就叫本原幂等元.

引理 1 设 R 是一个交换环，e 是 R 的一个本原幂等元. 那么 e 所生成的理想

$$eR=\{ea \mid a\in R\}$$

以 e 为单位元素，而在 eR 中除了 e 以外不再有其他的非零幂等元.

证. 显然 eR 以 e 为单位元素. 如果 e' 是 eR 中的一个非零幂等元，那么

$$e=e'+(e-e')$$

而

$$(e-e')^2=e-e'.\quad e'(e-e')=0.$$

因此 e 就分成两个互相正交的幂等元 e' 和 $e-e'$ 的和. 因 e 是本原幂等元，而 $e'\neq 0$，所以

$$e=e'.$$

定理 6 设 R 是一个有单位元素 1 的交换环，如果 1 可以表成有限个两两正交的本原幂等元的和，那么 R 就只有这有限个本原幂等元，因此 1 分解成有限个两两正交的本原幂等元的和的分解法，除本原幂等元的排列次序以外，是唯一的.

证. 设 1 分解成 r 个两两正交的本原幂等元 $e_1, e_2, \cdots, e_r$ 的和

$$1=e_1+e_2+\cdots+e_r$$

再设 e 是 R 的任意一个本原幂等元．将上式乘以 e，得

$$e=e_1e+e_2e+\cdots+e_re.$$

因 $e\neq 0$，所以至少有一个 i 使 $e_ie\neq 0$．那么

$$e=e_ie+(1-e_i)e.$$

显然

$$(e_ie)^2=e_i^2e^2=e_ie,$$

$$((1-e_i)e)^2=(1-e_i)^2e^2=(1-e_i)e,$$

$$(e_ie)\cdot(1-e_i)e=e_i(1-e_i)e^2=0.$$

即 e_ie 和 $(1-e_i)e$ 是两个互相正交的幂等元．因 e 是本原幂等元，而 $e_ie\neq 0$，所以

$$e=e_ie,\ (1-e_i)e=0.$$

但是 $e=e_ie\in e_iR$．根据引理 1，e_iR 只有 e_i 这唯一的一个非零幂等元，所以 $e=e_i$．这证明了 R 的本原幂等元必为 e_1，e_2，$\cdots$，e_r 中的一个．由此立刻推出，如不计本原幂等元的先后次序，那么 1 分解成有限个两两正交的本原幂等元的和的分解法是唯一的．

系理 在定理 6 的假设下，R 中任一非零幂等元 e 一定是某几个 e_i 的和．而且如不计本原幂等元的先后次序，那么 e 分解成本原幂等元的分解法是唯一的．

证． 设

$$1=e_1+e_2+\cdots+e_r, \tag{12}$$

其中 e_1，e_2，$\cdots$，e_r 是两两正交的本原幂等元．于是 R 就分解成 r 个理想 $R_i=e_iR$ $(i=1,\ 2,\ \cdots,\ r)$ 的直和

$$R=R_1\dot{+}R_2\dot{+}\cdots\dot{+}R_r. \tag{13}$$

设 e 是 R 的任一非零幂等元，将(12)式双方乘以 e，得

$$e=e_1e+e_2e+\cdots+e_re,$$

那么 $e_ie\in R_i$ 而 e_1e，e_2e，$\cdots$，e_re 是两两正交的幂等元．根据引理 1，$R_i=e_iR$ 中只有一个非零幂等元 e_i，所以

$$e_i e = e_i \quad 或\ 0.$$

这就证明了 e 是某几个 e_i 的和. 因 R 的本原幂等元只有 e_1, e_2, $\cdots$, e_r, 而(13)是直和分解,所以 e 表成本原幂等元的和的表示法是唯一的.

下面这个定理可以看作是定理 4 的逆定理.

定理 7 设 F 是一个域, $f(x)$是 $F[x]$中的一个次数 $\geqslant 1$ 的首项系数等于 1 的多项式, 假定 $F[x]_{f(x)}$ 的单位元素分解成 r 个两两正交的非零幂等元 e_1, e_2, $\cdots$, e_r 的和:

$$1 = e_1 \oplus e_2 \oplus \cdots \oplus e_r. \tag{14}$$

令

$$f_i(x) = (f(x),\ 1-e_i), \quad i=1,\ 2,\ \cdots,\ r, \tag{15}$$

那么 $f_1(x)$, $f_2(x)$, $\cdots$, $f_r(x)$ 是 r 个两两互素的次数 $\geqslant 1$ 的多项式,而

$$f(x) = f_1(x) f_2(x) \cdots f_r(x).$$

证. 先证明 $\partial^0 f_i(x) \geqslant 1$, 对 $i=1,\ 2,\ \cdots,\ r$. 由(15)式有

$$f_i(x) = a_i(x)(1-e_i) + b_i(x) f(x),$$
$$i=1,\ 2,\ \cdots,\ r,$$

其中 $a_i(x)$, $b_i(x) \in F[x]$. 那么在 $F[x]_{f(x)}$ 中

$$f_i(x) = (a_i(x))_{f(x)} \odot (1-e_i). \tag{16}$$

如果 $\partial^0 f_i(x) = 0$, 那么 $f_i(x) = 1$. 于是

$$1 = (a_i(x))_{f(x)} \odot (1-e_i),$$

将上式双方乘以 e_i, 就有

$$e_i = (a_i(x))_{f(x)} \odot (1-e_i) \odot e_i = (a_i(x))_{f(x)} \odot 0 = 0.$$

但 e_i 是非零幂等元,所以这不可能. 因此一定有

$$\partial^0 f_i(x) \geqslant 1, \quad 对\ i=1,\ 2,\ \cdots,\ r.$$

其次证明: 当 $i \neq j$ 时, $f_i(x)$ 与 $f_j(x)$ 互素. 设

$$d_{ij}(x) = (f_i(x),\ f_j(x)), \quad i \neq j.$$

显然 $\quad d_{ij}(x) \mid f(x), \quad d_{ij}(x) \mid 1-e_i, \quad d_{ij}(x) \mid 1-e_j.$

因 $e_i-e_j=(1-e_j)-(1-e_i)$，所以

$$d_{ij}(x)\mid e_i-e_j.$$

又因 $e_i\odot(e_i-e_j)=e_i$，所以

$$e_i=(e_i(e_i-e_j))_{f(x)}.$$

因此 $$d_{ij}(x)\mid e_i.$$

从 $d_{ij}(x)\mid 1-e_i$ 和 $d_{ij}(x)\mid e_i$ 推出 $d_{ij}(x)\mid 1$. 于是

$$d_{ij}(x)=1,$$

即 $$(f_i(x), f_j(x))=1, \quad 如果\ i\neq j.$$

从 $$f_i(x)\mid f(x),\ i=1, 2, \cdots, r,$$

以及 $f_1(x), f_2(x), \cdots, f_r(x)$ 两两互素，推出

$$f_1(x)f_2(x)\cdots f_r(x)\mid f(x). \tag{17}$$

另一方面，由(16)式推出

$$f_1(x)\odot f_2(x)\odot\cdots\odot f_r(x)=(a_1(x))_{f(x)}$$
$$\odot a_2(x)_{f(x)}\odot\cdots\odot(a_r(x))_{f(x)}\odot(1-e_1)$$
$$\odot(1-e_2)\odot\cdots\odot(1-e_r).$$

但

$$(1-e_1)\odot(1-e_2)\odot\cdots\odot(1-e_r)$$
$$=1-(e_1\oplus e_2\oplus\cdots\oplus e_r)=0,$$

所以 $$f_1(x)\odot f_2(x)\odot\cdots\odot f_r(x)=0,$$

即

$$f(x)\mid f_1(x)f_2(x)\cdots f_r(x). \tag{18}$$

由(17)，(18)两式就推出

$$f(x)=f_1(x)f_2(x)\cdots f_r(x).$$

这就证明了定理 7.

定理 8 设 F 是任意一个域，$f(x)$ 是 $F[x]$ 中一个次数 $\geqslant 1$ 的首项系数等于 1 的多项式，那么 $f(x)$ 分解成 $F[x]$ 中 r 个两两不同的不可约多项式的幂的乘积，当且仅当 $F[x]_{f(x)}$ 的单位元素 1 分解成 r 个两个正交的本原幂等元的和.

证. 设 $f(x)=p_1(x)^{b_1}p_2(x)^{b_2}\cdots p_r(x)^{b_r}$,
其中 $p_1(x), p_2(x), \cdots, p_r(x)$ 是 $F[x]$ 中 r 个两两不同的不可约多项式, 而 $b_1, b_2, \cdots, b_r$ 是 r 个正整数. 根据定理 4, $F[x]_{f(x)}$ 的单位元素 1 就分解成 r 个两两正交的非零幂等元 $e_1, e_2, \cdots, e_r$ 的和

$$1=e_1+e_2+\cdots+e_r.$$

我们要证明 $e_1, e_2, \cdots, e_r$ 都是本原幂等元. 假定 e_1 不是本原幂等元, 那么 e_1 可以分解成两个互相正交的非零幂等元 e_{11} 和 e_{12} 的和

$$e_1=e_{11}+e_{12}.$$

将上式乘以 e_{11}, 得

$$e_1e_{11}=e_{11}.$$

同理有

$$e_1e_{12}=e_{12}.$$

这就可以看出来 e_{11}, e_{12} 与 $e_2, e_3, \cdots, e_r$ 都正交, 因此 1 就分解成 $r+1$ 个两两正交的非零幂等元的和

$$1=e_{11}+e_{12}+e_2+\cdots+e_r.$$

再根据定理 7 就可以知道, $f(x)$ 将分解成 $r+1$ 个两两互素的次数 $\geqslant 1$ 的多项式的乘积, 但 $f(x)$ 只有 r 个两两互素的不可约因式 $p_1(x), p_2(x), \cdots, p_r(x)$. 这是一个矛盾. 因此 e_1 一定是本原幂等元. 同理可证 $e_2, e_3, \cdots, e_r$ 也都是本原幂等元.

反过来, 如果 $F[x]_{f(x)}$ 的单位元素 1 分解成 r 个两两正交的本原幂等元的和, 那么根据定理 6, $F[x]_{f(x)}$ 就只有这 r 个本原幂等元, 而根据定理 7, $f(x)$ 就分解成 r 个两两互素的次数 $\geqslant 1$ 的不可约多项式 $f_1(x), f_2(x), \cdots, f_r(x)$ 的乘积

$$f(x)=f_1(x)f_2(x)\cdots f_r(x).$$

我们要证明每个 $f_i(x)$ 都是 $F[x]$ 中不可约多项式的幂, 假定 $f_1(x)$ 不是不可约多项式的幂, 那么 $f_1(x)$ 就可以分解成两个

互素的次数 $\geqslant 1$ 的多项式 $f_{11}(x)$ 和 $f_{12}(x)$ 的乘积

$$f_1(x)=f_{11}(x)f_{12}(x).$$

这时 $f(x)$ 就分解成 $r+1$ 个两两互素的不可约多项式 $f_{11}(x)$, $f_{12}(x)$, $f_2(x)$, $f_3(x)$, $\cdots$, $f_r(x)$ 的乘积:

$$f(x)=f_{11}(x)f_{12}(x)f_2(x)f_3(x)\cdots f_r(x).$$

根据定理 4, $F[x]_{f(x)}$ 的单位元素 1 就分解成 $r+1$ 两两正交的非零幂等元的和. 根据定理 6 的系理, 每个非零幂等元都是 $F[x]_{f(x)}$ 的 r 个本原幂等元中某几个的和. 因此必有一个本原幂等元在两个互相正交的非零幂等元表成本原幂等元的和式中同时出现, 这是不可能的. 因此 $f_1(x)$ 一定是一个不可约多项式的幂. 同理可证 $f_2(x)$, $\cdots$, $f_r(x)$ 也都是不可约多项式的幂.

这证明了定理 8.

对于整数环 **Z** 中任一大于 1 的整数, 当然也可以叙述并证明平行于定理 7 和定理 8 的两条定理. 但由于今后并不用它们, 所以我们就不把它们写出来了.

第二章　线性代数初步

线性代数一般被认为是向量空间和线性变换的理论，有着丰富的内容和许多重要的应用．我们只准备介绍编码理论中所需要的一些线性代数的初步知识．这主要是向量空间的概念，矩阵的秩和矩阵的运算，线性方程组和行列式，多项式矩阵和矩阵在相似变换下的标准形．我们特别强调了用作用在矩阵的行上的初等变换将这个矩阵化成阶梯形矩阵这一方法；用这一方法去求矩阵的秩，并用这一方法去解线性方程组；这就是著名的消去法．我们只叙述了线性映射的定义，但没有对它进行讨论．我们关于行列式的介绍非常简略，这是因为估计读者都已熟悉它．如果读者对本章的介绍感到不够，请参看本书后面所附的参考书目中有关的书，特别是[2]或[4]或[14]的卷 II．

§1　向量空间的概念

我们回忆，三维欧几里得(Euclid)空间中的一个向量 $\mathbf{v}$，由它的三个分量，即它在三个坐标轴上的投影 v_1, v_2, v_3 所唯一确定．因此我们也记 $\mathbf{v}=(v_1, v_2, v_3)$．反过来，任给三个实数 v_1, v_2, v_3，也唯一确定一个向量 $\mathbf{v}$，它在三个坐标轴上的投影分别是 v_1, v_2, v_3．因此三维欧几里得空间中的向量 $\mathbf{v}$ 与三个实数组成的有序组 (v_1, v_2, v_3) 一一对应．三维欧几里得空间中的向量定义了向量的加法与用实数乘向量的乘法．设 $\mathbf{v}=(v_1, v_2, v_3)$ 和 $\mathbf{w}=(w_1, w_2, w_3)$ 是两个向量，那

么它们的和是

$$\mathbf{v}+\mathbf{w}=(v_1+w_1,\ v_2+w_2,\ v_3+w_3).$$

而用实数 c 乘向量 $\mathbf{v}$ 的乘积是

$$c\mathbf{v}=(cv_1,\ cv_2,\ cv_3).$$

我们也知道三维欧几里得空间中向量的加法满足下面这些运算规则:

I.1　对任意两个向量 $\mathbf{v}$ 和 $\mathbf{w}$, 有

$$\mathbf{v}+\mathbf{w}=\mathbf{w}+\mathbf{v}.$$

I.2　对任意三个向量 $\mathbf{v}$, $\mathbf{w}$ 和 $\mathbf{u}$, 有

$$(\mathbf{v}+\mathbf{w})+\mathbf{u}=\mathbf{v}+(\mathbf{w}+\mathbf{u}).$$

I.3　有一个向量(0, 0, 0), 记作 $\mathbf{0}$, 具有性质

$$\mathbf{v}+\mathbf{0}=\mathbf{v},\ \text{对任意向量 } \mathbf{v}.$$

I.4　对任意一个向量 $\mathbf{v}=(v_1,\ v_2,\ v_3)$, 都有一个向量 $(-v_1,\ -v_2,\ -v_3)$, 记作 $-\mathbf{v}$, 有性质

$$\mathbf{v}+(-\mathbf{v})=\mathbf{0}.$$

这就是说三维欧几里得空间中向量的全体对于向量的加法来说, 是一个交换群. 我们也知道用实数乘向量的乘法满足下面这些运算规则:

II.1　对任意实数 c 和向量 $\mathbf{v}$, $\mathbf{w}$, 都有

$$c(\mathbf{v}+\mathbf{w})=c\mathbf{v}+c\mathbf{w}.$$

II.2　对任意实数 c 和 d, 向量 $\mathbf{v}$, 都有

$$(c+d)\mathbf{v}=c\mathbf{v}+d\mathbf{v}.$$

II.3　对任意实数 c 和 d, 向量 $\mathbf{v}$, 都有

$$c(d\mathbf{v})=(cd)\mathbf{v}.$$

II.4　$1\cdot\mathbf{v}=\mathbf{v}$, 对任意向量 $\mathbf{v}$.

更进一步, 我们还知道,

III. 三维欧几里得空间中有三个向量

$$\mathbf{e}_1=(1,\ 0,\ 0),\ \mathbf{e}_2=(0,\ 1,\ 0),\ \mathbf{e}_3=(0,\ 0,\ 1)$$

使得任一向量 $\mathbf{v}=(v_1, v_2, v_3)$都可以表成它们的线性组合：

$$\mathbf{v}=v_1\mathbf{e}_1+v_2\mathbf{e}_2+v_3\mathbf{e}_3,$$

而且表法是唯一的.

三维欧几里得空间中的向量显然可以作如下的推广. 设 F 是任意一个域，而 n 是任意一个正整数. 考察 F 上的有序 n 元素组

$$(a_1, a_2, \cdots, a_n),\ a_i\in F,$$

的全体所组成的集合 $V_n(F)$，即

$$V_n(F)=\{(a_1, a_2, \cdots, a_n)\,|\,a_i\in F,\ i=1, 2, \cdots, n\}.$$

我们把 $V_n(F)$ 中的元素叫做向量并把 a_i 叫做向量$(a_1, a_2, \cdots, a_n)$的第 i 个分量. 在 $V_n(F)$ 中引进向量加法和用 F 中元素乘向量的乘法：

$$(a_1, a_2, \cdots, a_n)+(b_1, b_2, \cdots, b_n)$$
$$=(a_1+b_1, a_2+b_2, \cdots, a_n+b_n), \qquad (1)$$

$$c(a_1, a_2, \cdots, a_n)=(ca_1, ca_2, \cdots, ca_n),\ c\in F. \qquad (2)$$

显然 $V_n(F)$对于向量加法来说是一个交换群，即满足运算规则 I; $V_n(F)$ 中用 F 的元素去乘向量的乘法满足运算规则 II; 而 $V_n(F)$ 中有 n 个向量

$$\mathbf{e}_i=(0, 0, \cdots, 0, \underset{\text{第}i\text{个分量}}{1}, 0, \cdots, 0),\ i=1, 2, \cdots, n, \qquad (3)$$

使得 $V_n(F)$ 中任一向量$(a_1, a_2, \cdots, a_n)$可表成它们的线性组合：

$$(a_1, a_2, \cdots, a_n)=a_1\mathbf{e}_1+a_2\mathbf{e}_2+\cdots+a_n\mathbf{e}_n,$$

而且表法是唯一的.

从这些例子以及一些别的例子，我们归纳出向量空间的概念.

定义1 设F是一个域，V是一个非空集合．假定在V中规定了一个加法运算，即对于V中任意两个元素$\mathbf{v}$和$\mathbf{w}$，规定了它们的和$\mathbf{v}+\mathbf{w}$，并假定$\mathbf{v}+\mathbf{w}$仍是V中的元素，即V对于加法运算是自封的．再假定规定了一个用F中的元素去乘V中元素的运算，即对于$c\in F$和$\mathbf{v}\in V$，规定了$c\cdot\mathbf{v}$，并假定$c\cdot\mathbf{v}$仍是V中的元素．我们说V是F上的一个向量空间，如果V中的加法运算和用F的元素去乘V中元素的乘法运算满足以下运算规则：

I　V对于加法运算来说是一个交换群(这个交换群叫做V的加法群)．

II.1 对任意$c\in F$和$\mathbf{v}$，$\mathbf{w}\in V$，有

$$c\cdot(\mathbf{v}+\mathbf{w})=c\cdot\mathbf{v}+c\cdot\mathbf{w}.$$

II.2 对任意c，$d\in F$和$\mathbf{v}\in V$，有

$$(c+d)\cdot\mathbf{v}=c\cdot\mathbf{v}+d\cdot\mathbf{v}.$$

II.3 对任意c，$d\in F$和$\mathbf{v}\in V$，有

$$c(d\cdot\mathbf{v})=(cd)\cdot\mathbf{v}.$$

II.4 对任意$\mathbf{v}\in V$，有

$$1\cdot\mathbf{v}=\mathbf{v},$$

其中1是F的单位元素．

这时我们把V中元素叫做向量，并把V的加法群的零元素叫做零向量，记作$\mathbf{0}$，F中元素叫做纯量．

更进一步，如果以下条件成立：

III V中有n个向量$\mathbf{e}_1$，$\mathbf{e}_2$，…，$\mathbf{e}_n$使得V中任意一个向量$\mathbf{v}$都可以唯一地表成它们的线性组合

$$\mathbf{v}=c_1\mathbf{e}_1+c_2\mathbf{e}_2+\cdots+c_n\mathbf{e}_n,$$

而系数c_1，c_2，…，c_n都属于F，我们就说V是F上的有限维向量空间，而$\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$叫做$V$的一组基．

我们举几个例子．

例1 设 F 是任意一域，令

$$V_n(F)=\{(a_1, a_2, \cdots, a_n)\,|\,a_i\in F,\ i=1, 2, \cdots, n\}$$

那么 $V_n(F)$ 对于按照 (1) 式所规定的加法运算和按照 (2) 式所规定的用 F 的元素去乘 $V_n(F)$ 的元素的乘法运算来说是 F 上的一个有限维向量空间，而按 (3) 式规定的 $\mathbf{e}_i(i=1, 2, \cdots, n)$ 组成 $V_n(F)$ 的一组基 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$.

例2 设 F 是一个域，x 是一个文字，$F[x]$ 是 F 上一个文字 x 的多项式环. 我们知道 $F\subset F[x]$，因此用 F 的元素去乘 $F[x]$ 中的元素是有定义的. $F[x]$ 对于其中规定的加法运算和用 F 的元素去乘 $F[x]$ 中元素的乘法运算是 F 上的一个向量空间. 显然这个向量空间不满足 III.

例3 仍设 F 是一个域，$F[x]$ 是 F 上一个文字 x 的多项式环，而 $f(x)\in F[x]$. 更假定 $\partial^0 f(x)=n\geqslant 1$. 我们也知道 $F[x]_{f(x)}$ 是一个环，而 $F\subset F[x]_{f(x)}$. 因此用 F 的元素去乘 $F[x]_{f(x)}$ 的元素的乘法是有定义的. 这样，$F[x]_{f(x)}$ 对于其中规定的加法运算和用 F 的元素去乘 $F[x]_{f(x)}$ 的元素的乘法运算来说是一个向量空间. 更因 $F[x]_{f(x)}$ 中有 n 个元素，即 $1, x, x^2, \cdots, x^{n-1}$，使得 $F[x]_{f(x)}$ 中任一元素都可以唯一地表成它们的线性组合，而系数属于 F，所以 $F[x]_{f(x)}$ 是 F 上的有限维向量空间，而 $\{1, x, x^2, \cdots, x^{n-1}\}$ 是它的一组基.

例4 设 q 是一个素数 p 的幂，$q=p^n$，那么 $\mathbf{F}_q$ 包有素域 $\mathbf{F}_p$ 作为子域. 因此用 $\mathbf{F}_p$ 的元素去乘 $\mathbf{F}_q$ 的元素是有定义的. 这时 $\mathbf{F}_q$ 对于其中的加法运算和用 $\mathbf{F}_p$ 的元素去乘 $\mathbf{F}_q$ 的元素的乘法运算来说是 $\mathbf{F}_p$ 上的一个向量空间. 如果 ξ 是 $\mathbf{F}_q$ 的一个本原元，那么根据第一章 §5 定理 7，ξ 适合的 $\mathbf{F}_p$ 上的极小多项式就是 n 次不可约多项式. 这时 $\mathbf{F}_q$ 中每一个元素 α 都可以唯一地表成

$$\alpha=a_0+a_1\xi+a_2\xi^2+\cdots+a_{n-1}\xi^{n-1},$$

而系数 $a_0, a_1, a_2, \cdots, a_{n-1}$ 都属于 $\mathbf{F}_p$. 因此 $\mathbf{F}_q$ 是 $\mathbf{F}_p$ 上的有限维向量空间，而 $\{1, \xi, \cdots, \xi^{n-1}\}$ 是它的一组基.

更一般地，设 $\mathbf{F}_{q_0}$ 是 $\mathbf{F}_q$ 的子域，那么根据第一章 § 5 定理 4, $q=q_0^m$, 这时 $\mathbf{F}_q$ 可以看作是 $\mathbf{F}_{q_0}$ 上的有限维向量空间. 而第一章 § 5中给出的该定理的证明实际上就是找 F 的一组基.

例 5 设 V 是域 F 上的一个向量空间，而 S 是 V 的一个非空子集. 用 $[S]$ 表示 S 中任意的有限个向量 $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}$ 的线性组合 $c_1\mathbf{v}_{i_1}+c_2\mathbf{v}_{i_2}+\cdots+c_r\mathbf{v}_{i_r}$, $c_i\in F$ 的全体所组成的集合，即

$$[S]=\{c_1\mathbf{v}_{i_1}+c_2\mathbf{v}_{i_2}+\cdots+c_r\mathbf{v}_{i_r} \mid \mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}\in S,\ c_1, c_2, \cdots, c_r\in F\},$$

那么 $[S]$ 是 V 的子集. 设 $\mathbf{v}, \mathbf{w}\in[S]$, 它们作为 V 的元素，它们的和 $\mathbf{v}+\mathbf{w}$ 是有意义的，而且显然 $\mathbf{v}+\mathbf{w}\in[S]$. 我们把 $\mathbf{v}$ 和 $\mathbf{w}$ 按 V 中加法运算所得之和 $\mathbf{v}+\mathbf{w}$ 看作是它们作为 $[S]$ 中元素的和. 同样，对 $c\in F$ 和 $\mathbf{v}\in[S]$, 将 $\mathbf{v}$ 看作 V 中元素，规定了 $c\cdot\mathbf{v}$. 显然 $c\cdot\mathbf{v}\in[S]$. 我们把 $\mathbf{v}$ 看作 V 中元素规定的乘积 $c\cdot\mathbf{v}$ 看作是把 $\mathbf{v}$ 看作 $[S]$ 中元素规定的乘积. 那么容易证明，$[S]$ 对于这样规定的运算是一个向量空间，叫做由 S 生成的向量空间. 当 S 是 V 的一个有限子集时，譬如 $S=\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r\}$, 我们也记 $[S]=[\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r]$.

特别，设 V 是 F 上的有限维向量空间，而 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ 是 V 的一组基，那么从 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 中任取 $r(\leqslant n)$ 个: $\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \cdots, \mathbf{e}_{i_r} (1\leqslant i_1<i_2<\cdots<i_r\leqslant n)$, 它们生成一个向量空间

$$[\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \cdots, \mathbf{e}_{i_r}] =\{c_1\mathbf{e}_{i_1}+c_2\mathbf{e}_{i_2}+\cdots+c_r\mathbf{e}_{i_r} \mid c_1, c_2, \cdots, c_r\in F\}.$$

而 $\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \cdots, \mathbf{e}_{i_r}$ 就是 $[\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \cdots, \mathbf{e}_{i_r}]$ 的一组基.

我们先证明

定理 1 设 V 是域 F 的一个向量空间，那么以下运算规则成立：

i) $0\cdot\mathbf{v}=\mathbf{0}$. 对任意 $\mathbf{v}\in V$.

ii) $c\cdot\mathbf{0}=\mathbf{0}$, 对任意 $c\in V$.

iii) $(-1)\cdot\mathbf{v}=-\mathbf{v}$, 对任意 $\mathbf{v}\in V$.

iv) 如果 $c\cdot\mathbf{v}=\mathbf{0}$，那么 $c=0$ 或 $\mathbf{v}=\mathbf{0}$.

证. 我们有

$$0\cdot\mathbf{v}=(0+0)\cdot\mathbf{v}=0\cdot\mathbf{v}+0\cdot\mathbf{v}.$$

因 V 对向量加法是交换群，根据消去律就有

$$0\cdot\mathbf{v}=\mathbf{0},$$

这证明了 i) 成立. 同理可证 ii) 成立.

又有
$$\mathbf{v}+(-\mathbf{v})=\mathbf{0}=0\cdot\mathbf{v}=(1+(-1))\mathbf{v}$$
$$=\mathbf{v}+(-1)\mathbf{v}.$$

仍根据消去律，就有

$$(-1)\mathbf{v}=-\mathbf{v},$$

这证明了 iii) 成立.

最后，设
$$c\cdot\mathbf{v}=\mathbf{0}.$$
如果 $c\neq 0$，将上式双方乘以 c^{-1} 就有

$$\mathbf{0}=c^{-1}\cdot\mathbf{0}=c^{-1}(c\cdot\mathbf{v})=(c^{-1}c)\cdot\mathbf{v}=1\cdot\mathbf{v}=\mathbf{v},$$

因此 iv) 也成立.

一个自然发生的问题是，向量空间中不同的两组基所含向量的个数是不是相等的？这个问题的答案是肯定的. 为了解决这个问题，需要引进向量的线性相关这一重要概念. 这个概念可以看作三维欧几里得空间中向量的共线或共面概念的推广.

定义 2 设 V 是域 F 上的一个向量空间，而 $\mathbf{v}_1$, $\mathbf{v}_2$, …,

$\mathbf{v}_r$ 是 V 中 r 个向量．我们说 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性相关，如果 F 中有 r 个不全等于 0 的元素 $c_1, c_2, \cdots, c_r$ 使

$$c_1\mathbf{v}_1+c_2\mathbf{v}_2+\cdots+c_r\mathbf{v}_r=\mathbf{0}. \tag{4}$$

这时 (4) 式叫做 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 的一个非零线性关系．如果 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 不线性相关，即如果 F 中有 r 个元素 $c_1, c_2, \cdots, c_r$ 使(4)式成立，那么一定有 $c_1=c_2=\cdots=c_r=0$，我们就说 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_2$ 线性无关．

从这个定义立刻推出

定理 2 设 V 是域 F 上的有限维向量空间，那么 V 的任意一组基中的向量都线性无关．

证．设$\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$是 V 的一组基．如果 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 线性相关，即有 F 中的 n 个不全为 0 的元素 $c_1, c_2, \cdots, c_n$ 使

$$c_1\mathbf{e}_1+c_2\mathbf{e}_2+\cdots+c_n\mathbf{e}_n=\mathbf{0}.$$

这时，$\mathbf{0}$ 就有两种方法表成 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 的线性组合：

$$\begin{aligned}\mathbf{0}&=0\cdot\mathbf{e}_1+0\cdot\mathbf{e}_2+\cdots+0\cdot\mathbf{e}_n\\&=c_1\mathbf{e}_1+c_2\mathbf{e}_2+\cdots+c_n\mathbf{e}_n.\end{aligned}$$

这与$\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$是 V 的一组基的假设相矛盾．

我们再证明下面几个引理．

引理 1 如果 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性相关，那么 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{v}_{r+1}$ 也线性相关．

证．设 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性相关，即 F 中有不全等于 0 的 r 个元素 $c_1, c_2, \cdots, c_r$ 使

$$c_1\mathbf{v}_1+c_2\mathbf{v}_2+\cdots+c_r\mathbf{v}_r=\mathbf{0},$$

那么
$$c_1\mathbf{v}_1+c_2\mathbf{v}_2+\cdots+c_r\mathbf{v}_r+0\cdot\mathbf{v}_{r+1}=\mathbf{0}.$$

自然 $c_1, c_2, \cdots, c_r$, 0 不全等于 0．因此 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{r+1}$ 线性相关．

引理 2 如果 $\mathbf{v}_{r+1}$ 可以表成 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 的线性组合，那么 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{v}_{r+1}$ 线性相关.

证. 设

$$\mathbf{v}_{r+1}=c_1\mathbf{v}_1+c_2\mathbf{v}_2+\cdots+c_r\mathbf{v}_r,\ c_i\in F,$$

那么 $$c_1\mathbf{v}_1+c_2\mathbf{v}_2+\cdots+c_r\mathbf{v}_r+(-1)\mathbf{v}_{r+1}=\mathbf{0},$$

就是 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{v}_{r+1}$ 的一个非零线性关系. 因此 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{v}_{r+1}$ 线性相关.

引理 3 如果 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性无关，而 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{v}_{r+1}$ 线性相关，那么 $\mathbf{v}_{r+1}$ 可以唯一地表成 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 的线性组合，而系数属于 F，即

$$\mathbf{v}_{r+1}=c_1\mathbf{v}_1+c_2\mathbf{v}_2+\cdots+c_r\mathbf{v}_r,\ c_i\in F,$$

而 $c_1, c_2, \cdots, c_r$ 由 $\mathbf{v}_{r+1}$ 唯一确定.

证. 因 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{v}_{r+1}$ 线性相关，故 F 中有 $r+1$ 不全等于 0 的元素 $a_1, a_2, \cdots, a_r, a_{r+1}$ 使

$$a_1\mathbf{v}_1+a_2\mathbf{v}_2+\cdots+a_r\mathbf{v}_r+a_{r+1}\mathbf{v}_{r+1}=\mathbf{0}. \tag{5}$$

因 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性无关，所以 $a_{r+1}\neq 0$；否则设 $a_{r+1}=0$，那么 $a_1, a_2, \cdots, a_r$ 就不全等于 0，这样 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 就有一个非零线性关系 $a_1\mathbf{v}_1+a_2\mathbf{v}_2+\cdots+a_r\mathbf{v}_r=\mathbf{0}$. 既然 $a_{r+1}\neq 0$，由(5)式得到

$$\begin{aligned}\mathbf{v}_{r+1}=&(-a_{r+1}^{-1}a_1)\mathbf{v}_1+(-a_{r+1}^{-1}a_2)\mathbf{v}_2\\&+\cdots+(-a_{r+1}^{-1}a_r)\mathbf{v}_r,\end{aligned}$$

而 $-a_{r+1}^{-1}a_i\in F,\ i=1, 2, \cdots, r$.

更进一步，如果 $\mathbf{v}_{r+1}$ 有两种方法表成 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 的线性组合

$$\mathbf{v}_{r+1}=c_1\mathbf{v}_1+c_2\mathbf{v}_2+\cdots+c_r\mathbf{v}_r,\ c_i\in F,$$

$$\mathbf{v}_{r+1}=d_1\mathbf{v}_1+d_2\mathbf{v}_2+\cdots+d_r\mathbf{v}_r,\ d_i\in F.$$

将上面两个式子相减就得到

$$\mathbf{0}=(c_1-d_1)\mathbf{v}_1+(c_2-d_2)\mathbf{v}_2+\cdots+(c_r-d_r)\mathbf{v}_r.$$

因 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性无关，所以一定有

$$c_1-d_1=c_2-d_2=\cdots=c_r-d_r=0,$$

于是
$$c_i=d_i,\ i=1,\ 2,\ \cdots,\ r,$$

这证明了表法的唯一性.

引理 4 如果 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 中有一个向量是 $\mathbf{0}$, 那么它们一定线性相关.

证. 设 $\mathbf{v}_1=\mathbf{0}$, 那么

$$1\cdot\mathbf{v}_1+0\cdot\mathbf{v}_2+0\cdot\mathbf{v}_3+\cdots+0\cdot\mathbf{v}_r=\mathbf{0},$$

就是 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 的一个非零线性关系，因此它们线性相关.

引理 5 设 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 是 r 个向量而 $r>1$, 令

$$\mathbf{v}_i'=\mathbf{v}_i+a_i\mathbf{v}_1,\ a_i\in F,\ i>1,$$

那么 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性无关，当且仅当 $\mathbf{v}_1, \mathbf{v}_2', \cdots, \mathbf{v}_r'$ 线性无关.

证. 设 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性无关. 假定有 $c_1, c_2, \cdots, c_r\in F$ 使

$$c_1\mathbf{v}_1+c_2\mathbf{v}_2'+c_3\mathbf{v}_3'+\cdots+c_r\mathbf{v}_r'=\mathbf{0}.$$

将 $\mathbf{v}_i'=\mathbf{v}_i+a_i\mathbf{v}_1\ (i=2,\ 3,\ \cdots,\ r)$ 代入上式得

$$(c_1+c_2a_2+c_3a_3+\cdots+c_ra_r)\mathbf{v}_1+c_2\mathbf{v}_2$$
$$+c_3\mathbf{v}_3+\cdots+c_r\mathbf{v}_r=\mathbf{0}.$$

因 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性无关，所以

$$c_1+c_2a_2+c_3a_3+\cdots+c_ra_r=0,$$
$$c_2=c_3=\cdots=c_r=0.$$

因此也有 $c_1=0$. 这证明了 $\mathbf{v}_1, \mathbf{v}_2', \mathbf{v}_3', \cdots, \mathbf{v}_r'$ 没有非零线性关系，因此它们线性无关.

反过来，$\mathbf{v}_i=\mathbf{v}_i'+(-a_i)\mathbf{v}_1\ (i>1)$. 所以从 $\mathbf{v}_1, \mathbf{v}_2', \mathbf{v}_3', \cdots, \mathbf{v}_r'$ 线性无关也可以推出 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r$ 线性无关.

定理 3 设 V 是域 F 上的有限维向量空间，它有一组基由 n 个向量组成，而 $m>n$，那么 V 中任意 m 个向量都线性相关。

证．根据引理 1，只要证明 V 中任意 $n+1$ 个向量都线性相关即可．我们对 n 用归纳法来证明这一点．

设 $n=1$，而 $\{\mathbf{e}_1\}$ 是 V 的一组基，再设 $\mathbf{v}_1$, $\mathbf{v}_2$ 是 V 中任意两个向量，那么 $\mathbf{v}_1=a_1\mathbf{e}_1$, $\mathbf{v}_2=a_2\mathbf{e}_1$. 如果 $\mathbf{v}_1=\mathbf{0}$，根据引理 4, $\mathbf{v}_1$, $\mathbf{v}_2$ 线性相关．如果 $\mathbf{v}_1\neq\mathbf{0}$，根据定理 1, $a_1\neq 0$. 那么

$$(-a_2)\mathbf{v}_1+a_1\mathbf{v}_2=\mathbf{0}.$$

就是 $\mathbf{v}_1$, $\mathbf{v}_2$ 的一个非零线性关系，因此 $\mathbf{v}_1$, $\mathbf{v}_2$ 也线性相关．

假定任一有限维向量空间如有一组基由 $n-1$ 个向量组成，其中任意 n 个向量都线性相关．设 V 是有限维向量空间，而 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ 是 V 的一组基．再设 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{n+1}$ 是 V 中任意 $n+1$ 个向量，那么

$$\mathbf{v}_1=a_{11}\mathbf{e}_1+a_{12}\mathbf{e}_2+\cdots+a_{1n}\mathbf{e}_n,$$
$$\mathbf{v}_2=a_{21}\mathbf{e}_1+a_{22}\mathbf{e}_2+\cdots+a_{2n}\mathbf{e}_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathbf{v}_{n+1}=a_{n+11}\mathbf{e}_1+a_{n+12}\mathbf{e}_2+\cdots+a_{n+1n}\mathbf{e}_n,$$

而 $a_{ij}\in F$, $i=1, 2, \cdots, n+1$, $j=1, 2, \cdots, n$. 根据引理 4，不妨设 $\mathbf{v}_1\neq\mathbf{0}$，那么一定有一个 $a_{1i}\neq 0$. 设 $a_{11}\neq 0$. 令

$$\mathbf{v}_i'=\mathbf{v}_i-a_{i1}a_{11}^{-1}\mathbf{v}_1,\ i=2, 3, \cdots, n+1.$$

根据引理 5，要证 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{n+1}$ 线性相关，只要证 $\mathbf{v}_1, \mathbf{v}_2', \cdots, \mathbf{v}_{n+1}'$ 线性相关就行了．注意

$$\mathbf{v}_i'=(a_{i2}-a_{i1}a_{11}^{-1}a_{12})\mathbf{e}_2+\cdots+(a_{in}-a_{i1}a_{11}^{-1}a_{1n})\mathbf{e}_n,$$
$$i=2, 3, \cdots, n+1.$$

因此 $\mathbf{v}_2', \mathbf{v}_3', \cdots, \mathbf{v}_{n+1}'$ 是 $[\mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_n]$ 中的 n 个向量．显然 $[\mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_n]$ 是 F 上的有限维向量空间，而 $\{\mathbf{e}_2, \mathbf{e}_3, \cdots,$

$\mathbf{e}_n\}$ 是 $[\mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_n]$ 的一组基. 根据归纳法假设, $\mathbf{v}_2'$, $\mathbf{v}_3'$, $\cdots$, $\mathbf{v}_{n+1}'$ 线性相关. 再根据引理 1, $\mathbf{v}_1$, $\mathbf{v}_2'$, $\mathbf{v}_3'$, $\cdots$, $\mathbf{v}_{n+1}'$ 也线性相关, 最后根据引理5, $\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_{n+1}$ 线性相关.

这证明了定理 3.

系理1 设 V 是 F 上的有限维向量空间, 那么它的任意两组基都含相同个数的向量.

证. 设 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ 和 $\{\mathbf{e}_1', \mathbf{e}_2', \cdots, \mathbf{e}_m'\}$ 是 V 的两组基. 根据定理 3, 一方面有 $m \leqslant n$, 另一方面 $n \leqslant m$, 所以 $n=m$.

基于系理 1 我们可以给出下面的定义.

定义3 设 V 是 F 上的有限维向量空间. 如果 V 有一组由 n 个向量组成的基, V 就叫 F 上的 n 维向量空间, 记作 $\dim V=n$. 如果 V 仅由零向量组成, 我们就说 V 是 0 维的, 记作 $\dim V=0$.

系理2 设 V 是 F 上的 n 维向量空间, 那么 V 中任意 n 个线性无关的向量都组成 V 的一组基.

证. 设 $\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_n$ 是 V 的 n 个线性无关的向量. 再设 $\mathbf{v}$ 是 V 中任意一个向量. 根据定理 3, $\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_n$, $\mathbf{v}$ 一定线性相关. 再根据引理 3, $\mathbf{v}$ 可以唯一地表成 $\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_n$ 的线性组合. 因此$\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$是 V 的一组基.

系理3 设 V 是域 F 上的 n 维向量空间, 而 $\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_r$ 是 V 中 r 个线性无关的向量, $r \leqslant n$, 那么可以从 V 的一组基$\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$中选出 $n-r$ 个向量, 它们和$\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_r$ 一起就组成 V 的一组基.

证. 考察向量集合 $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$. 从其中选一个包有 $\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_r$ 的极大的线性无关的向量子集 $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \mathbf{e}_{k_{r+2}}, \cdots, \mathbf{e}_{k_m}\}$. 这就是说 $\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_r$, $\mathbf{e}_{k_{r+1}}$, $\mathbf{e}_{k_{r+2}}$, $\cdots$, $\mathbf{e}_{k_m}$ 是线性无关的, 而 $\mathbf{v}_1$, $\mathbf{v}_2$, $\cdots$, $\mathbf{v}_r$, $\mathbf{e}_{k_{r+1}}$,

$\mathbf{e}_{k_{r+2}}, \cdots, \mathbf{e}_{k_m}, \mathbf{e}_j(j\neq k_{r+1}, k_{r+2}, \cdots, k_m)$都线性相关．那么根据引理2，$\mathbf{e}_j(j\neq k_{r+1}, k_{r+2}, \cdots, k_m)$就可以表成$\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \mathbf{e}_{k_{r+2}}, \cdots, \mathbf{e}_{k_m}$的线性组合．显然$\mathbf{e}_{k_{r+1}}, \mathbf{e}_{k_{r+2}}, \cdots, \mathbf{e}_{k_m}$也都可以表成它们的线性组合．这证明了$\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$都可以表成$\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \mathbf{e}_{k_{r+2}}, \cdots, \mathbf{e}_{k_m}$的线性组合．

设$\mathbf{v}$是V中任一向量．因$\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$是一组基，所以$\mathbf{v}$可以表成$\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$的线性组合：

$$\mathbf{v}=c_1\mathbf{e}_1+c_2\mathbf{e}_2+\cdots+c_n\mathbf{e}_n,\ c_i\in F. \tag{6}$$

刚才已经证明，每个$\mathbf{e}_i(1\leqslant i\leqslant n)$都可以表成$\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \mathbf{e}_{k_{r+2}}, \cdots, \mathbf{e}_{k_m}$的线性组合．将每个$\mathbf{e}_i$表成$\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \cdots, \mathbf{e}_{k_m}$的线性组合的表示式代入(6)，就将$\mathbf{v}$表成$\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \cdots, \mathbf{e}_{k_m}$的线性组合．那么根据引理2，$\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \cdots, \mathbf{e}_{k_m}, \mathbf{v}$线性相关．再根据引理3，$\mathbf{v}$可以唯一地表成$\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \cdots, \mathbf{e}_{k_m}$的线性组合．因此$\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_r, \mathbf{e}_{k_{r+1}}, \cdots, \mathbf{e}_{k_m}\}$是$V$的一组基．再根据系理1，$m=n$．

设V是域F上的向量空间．S是V的一个有限子集．在例5中已经指出，S生成的向量空间$[S]$中的运算实际上就是V中的运算，这启发我们给出下面的定义．

定义4 设V是域F上的向量空间，而W是V的一个非空子集．如果W对于V中规定的加法运算和用F的元素去乘V的元素的乘法运算来说，也是F上的一个向量空间，那么W就叫V的一个子空间．

特别，当S是V的一个有限子集时，$[S]$叫做由S生成的子空间．

为了验证向量空间V的一个非空子集是否子空间，应用下面的定理中给出的条件是方便的．

定理4 设V是域F上的一个向量空间，而W是V的

一个非空子集，那么 W 是 V 的子空间，当且仅当以下两个条件成立：

i) 对任意 $\mathbf{w}_1, \mathbf{w}_2 \in W$，都有 $\mathbf{w}_1+\mathbf{w}_2 \in W$。

ii) 对任意 $c \in F$, $\mathbf{w} \in W$，都有 $c\mathbf{w} \in W$。

证．当 W 是子空间时，显然 i)，ii) 成立．

反之，设 W 是 V 的非空子集，而条件 i)，ii) 成立，那么对任意 $\mathbf{w} \in W$，根据 ii) $-\mathbf{w}=(-1)\mathbf{w} \in W$．再根据 i) 就有 $\mathbf{0}=\mathbf{w}+(-\mathbf{w}) \in W$．这些说明了 W 对于 V 中加法运算来说是 V 的子群．因此 I 在 W 中成立．至于 II 在 W 中成立是显然的．因此 W 是 V 的子空间．

我们还有

定理 5 设 V 是域 F 上的一个 n 维向量空间，而 W 是 V 的一个子空间．那么 $\dim W \leqslant \dim V$，而等号成立当且仅当 $W=V$。

证．根据定理 3，W 中任意 $n+1$ 个向量都线性相关．设 $\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_m$ 是 W 中一个极大的线性无关的向量组，即 $\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_m$ 线性无关，而如果 $\mathbf{w}$ 是 W 中任一向量，$\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_m, \mathbf{w}$ 就线性相关．于是 $m \leqslant n$．根据引理 3，W 中任一向量都可以唯一地表成 $\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_m$ 的线性组合．因此 $\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_m$ 就是 W 的一组基．因此，$\dim W \leqslant \dim V$，再根据定理 3 的系理 3，当 $m=n$ 时，$\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_m$ 就是 V 的一组基，那么 V 中任一向量都可以表成它们的线性组合，因此 $V \subset W$．于是 $V=W$．

我们再证明

定理 6 设 V 是域 F 上的一个向量空间，而 W 是 V 的一个子空间，那么 W 是 V 的加法群的子群，于是 V 就分成 W 的一些两两没有公共元素的倍集 $\mathbf{v}+W$ 的并．用 V/W 表示两两没有公共元素的 W 的陪集所组成的集合而它们的并

是 V, 那么 V/W 对于如下规定的加法运算

$$(\mathbf{v}_1+W)+(\mathbf{v}_2+W)=(\mathbf{v}_1+\mathbf{v}_2)+W,$$

$$\text{对任意 } \mathbf{v}_1+W,\ \mathbf{v}_2+W\in V/W$$

是一个交换群. 更进一步, 对任意 $c\in F$, $\mathbf{v}+W$, 规定

$$c\cdot(\mathbf{v}+W)=c\cdot\mathbf{v}+W, \tag{7}$$

那么 V/W 就是 F 上的一个向量空间.

证. 在第一章 §7 定理 1 里已经证明 V/W 是交换群. 现在证明按 (7) 规定的用 F 的元素去乘 V/W 的元素的乘法运算与陪集的代表元的选择无关. 设 $\mathbf{v}'\in\mathbf{v}+W$, 那么 $\mathbf{v}'=\mathbf{v}+\mathbf{w}$. 于是

$$\begin{aligned} c\cdot(\mathbf{v}'+W)&=c\cdot\mathbf{v}+W=c\cdot(\mathbf{v}+\mathbf{w})+W=c\cdot\mathbf{v}+c\mathbf{w}+W\\ &=c\cdot\mathbf{v}+W=c\cdot(\mathbf{v}+W). \end{aligned}$$

从 V 中 II 成立, 容易推出 V/W 中 II 也成立. 例如, 我们来验证在 V/W 中 II.1 成立:

$$\begin{aligned} c\cdot[(\mathbf{v}_1+W)+(\mathbf{v}_2+W)]&=c\cdot[(\mathbf{v}_1+\mathbf{v}_2)+W]\\ &=c\cdot(\mathbf{v}_1+\mathbf{v}_2)+W=c\cdot\mathbf{v}_1+c\cdot\mathbf{v}_2+W\\ &=(c\cdot\mathbf{v}_1+W)+(c\cdot\mathbf{v}_2+W)\\ &=c\cdot(\mathbf{v}_1+W)+c\cdot(\mathbf{v}_2+W). \end{aligned}$$

这样就证明了 V/W 是 F 上的一个向量空间.

定义 5 设 V 是域 F 上的向量空间, 而 W 是 V 的一个子空间. V/W 叫做 V 对于 W 的商空间.

我们再引进向量空间的直和分解的定义.

定义 6 设 V 是域 F 上的向量空间, 而 V_1, V_2, $\cdots$, V_r 都是 V 的子空间. 如果 V 中任一元素 $\mathbf{v}$ 都可以唯一地表成 V_1 中一个元素, V_2 中一个元素, $\cdots$ 和 V_r 中一个元素的和, 我们就说 V 分解成了 V_1, V_2, $\cdots$, V_r 的直和, 记作

$$V=V_1\dot{+}V_2\dot{+}\cdots\dot{+}V_r.$$

例如, 当 V 是域 F 上的 n 维向量空间而 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$

是它的一组基时，V 就分解成了子空间 $[\mathbf{e}_1]$，$[\mathbf{e}_2]$，…，$[\mathbf{e}_n]$ 的直和：

$$V=[\mathbf{e}_1]\dot{+}[\mathbf{e}_2]\dot{+}\cdots\dot{+}[\mathbf{e}_n].$$

又如，设 $f(x)$ 是 $F[x]$ 中的一个次数 $\geqslant 1$ 的多项式，而

$$f(x)=f_1(x)f_2(x)\cdots f_r(x).$$

其中 $f_1(x)$，$f_2(x)$，…，$f_r(x)$ 是 r 个两两互素的多项式．根据第一章§8定理4，我们有交换环 $F[x]_{f(x)}$ 的直和分解：

$$F[x]_{f(x)}=F[x]'_{f_1(x)}\dot{\oplus}F[x]'_{f_2(x)}\dot{\oplus}\cdots\dot{\oplus}F[x]'_{f_r(x)}. \tag{8}$$

其中 $F[x]'_{f_i(x)}$ $(1\leqslant i\leqslant r)$ 都是 $F[x]_{f(x)}$ 的理想．但 $F[x]_{f(x)}$ 是 F 上的向量空间，而 $F[x]'_{f_i(x)}$ $(1\leqslant i\leqslant r)$ 显然是 $F[x]_{f(x)}$ 的子空间．因此(8)也是向量空间 $F[x]_{f(x)}$ 的一个直和分解．

和域的同构一样，我们也可以引进向量空间的同构的概念．

定义7 设 V 和 V' 是域 F 上的两个向量空间．从 V 映到 V' 之上的一个一一映射 σ

$$\sigma: V\to V'$$

就做从 V 到 V' 的一个同构映射，或简称同构，如果 σ 适合下面两个条件：

i) 对 V 中任意两个向量 $\mathbf{v}_1$，$\mathbf{v}_2$，都有

$$\sigma(\mathbf{v}_1+\mathbf{v}_2)=\sigma(\mathbf{v}_1)+\sigma(\mathbf{v}_2)$$

ii) 对 V 中任意一个向量 $\mathbf{v}$，和 F 中任意一个元素 c，都有

$$\sigma(c\mathbf{v})=c\sigma(\mathbf{v}).$$

这时我们就说 V 和 V' 同构．

我们先证明

定理7 同一个域 F 上的两个同构的有限维向量空间有相同的维数．

证．设 V 和 V' 是 F 上的两个同构的有限维向量空间．

并假定

$$\sigma: V \to V'$$

是从 V 到 V' 之上的一个同构. 再设 $\dim V = n$, $\dim V' = m$, 那么 V 有一组基, 它由 n 个向量 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 组成. 我们来证明 $\sigma(\mathbf{e}_1), \sigma(\mathbf{e}_2), \cdots, \sigma(\mathbf{e}_n)$ 在 F 上线性无关. 设有线性关系

$$c_1\sigma(\mathbf{e}_1) + c_2\sigma(\mathbf{e}_2) + \cdots + c_n\sigma(\mathbf{e}_n) = \mathbf{0}, \quad c_i \in F.$$

因 σ 是同构, 所以

$$\begin{aligned}&\sigma(c_1\mathbf{e}_1 + c_2\mathbf{e}_2 + \cdots + c_n\mathbf{e}_n)\\ &= c_1\sigma(\mathbf{e}_1) + c_2\sigma(\mathbf{e}_2) + \cdots + c_n\sigma(\mathbf{e}_n) = \mathbf{0}.\end{aligned}$$

仍因 σ 是同构, σ 是一一映射, 所以

$$c_1\mathbf{e}_1 + c_2\mathbf{e}_2 + \cdots + c_n\mathbf{e}_n = \mathbf{0}.$$

因 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 是一组基, 所以

$$c_1 = c_2 = \cdots = c_n = \mathbf{0}.$$

这证明了 $\sigma(\mathbf{e}_1), \sigma(\mathbf{e}_2), \cdots, \sigma(\mathbf{e}_n)$ 线性无关. 根据定理 3, $n \leqslant m$. 同理可证 $m \leqslant n$. 所以 $n = m$.

我们还有

定理 8 设 V 是域 F 上的一个 n 维向量空间, 那么 V 一定和 $V_n(F)$ 同构.

证. 设 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ 是 V 的一组基, 那么 V 中任意一个向量 $\mathbf{v}$ 都可以唯一地表成 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 的线性组合

$$\mathbf{v} = v_1\mathbf{e}_1 + v_2\mathbf{e}_2 + \cdots + v_n\mathbf{e}_n, \quad v_i \in F,$$

那么 $\mathbf{v}$ 就唯一地确定了 $V_n(F)$ 中的一个向量 $(v_1, v_2, \cdots, v_n)$. 反过来, $\mathbf{v}$ 又由 $(v_1, v_2, \cdots, v_n)$ 唯一确定. 这样就定义了一个从 V 到 $V_n(F)$ 之上的一一映射

$$\sigma: \mathbf{v} \to (v_1, v_2, \cdots, v_n).$$

再设 $\mathbf{w} \in V$, 那么 $\mathbf{w}$ 也可以唯一地表成 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 的线性组合

$$\mathbf{w}=w_1\mathbf{e}_1+w_2\mathbf{e}_2+\cdots+w_n\mathbf{e}_n,$$

于是

$$\mathbf{v}+\mathbf{w}=(v_1+w_1)\mathbf{e}_1+(v_2+w_2)\mathbf{e}_2+\cdots+(v_n+w_n)\mathbf{e}_n,$$

因此

$$\begin{aligned}\sigma(\mathbf{v}+\mathbf{w})&=(v_1+w_1,\ v_2+w_2,\ \cdots,\ v_n+w_n)\\&=(v_1,\ v_2,\ \cdots,\ v_n)+(w_1,\ w_2,\ \cdots,\ w_n)\\&=\sigma(\mathbf{v})+\sigma(\mathbf{w}).\end{aligned}$$

设 $c\in F$, 那么

$$\begin{aligned}c\mathbf{v}&=c(v_1\mathbf{e}_1+v_2\mathbf{e}_2+\cdots+v_n\mathbf{e}_n)\\&=(cv_1)\mathbf{e}_1+(cv_2)\mathbf{e}_2+\cdots+(cv_n)\mathbf{e}_n,\end{aligned}$$

因此

$$\begin{aligned}\sigma(c\mathbf{v})&=(cv_1,\ cv_2,\ \cdots,\ cv_n)\\&=c(v_1,\ v_2,\ \cdots,\ v_n)=c\sigma(\mathbf{v}).\end{aligned}$$

这证明了 σ 是个同构.

根据定理 8 可以说，对于有限维向量空间来说，只讨论 $V_n(F)$并不失普遍性.

§2 矩阵和它的秩

设 V 是域 F 上的一个向量空间，S 是 V 的一个有限子集,那么$[S]$是 V 的子空间,设

$$S=\{\mathbf{v}_1,\ \mathbf{v}_2,\ \cdots,\ \mathbf{v}_m\}.$$

S 的一个子集

$$S_0=\{\mathbf{v}_{i_1},\ \mathbf{v}_{i_2},\ \cdots,\ \mathbf{v}_{i_r}\,|\,1\leqslant i_1<i_2<\cdots<i_r\leqslant m\}$$

叫做 S 的一个极大线性无关子集，如果 $\mathbf{v}_{i_1}$, $\mathbf{v}_{i_2}$, $\cdots$, $\mathbf{v}_{i_r}$ 线性无关，而 S 中任一向量（或任一不属于 S_0 的向量）都可以表成 $\mathbf{v}_{i_1}$, $\mathbf{v}_{i_2}$, $\cdots$, $\mathbf{v}_{i_r}$ 的线性组合．我们先证明

定理 1 设 V 是域 F 上的一个向量空间,S 是 V 的一个

有限子集，而 S_0 是 S 的一个极大线性无关子集，那么 $\dim[S] = |S_0|$，这里 $|S_0|$ 表示 S_0 中的元素个数.

证. 设 $S=\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}$，而 $S_0=\{\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}\}$ $(1\leqslant i_1<i_2<\cdots<i_r\leqslant m)$. 因 $[S]$ 中任一向量都是 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m$ 的线性组合，而每个 $\mathbf{v}_i(1\leqslant i\leqslant m)$ 都可以表成 $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}$ 的线性组合，所以 $[S]$ 中任一向量都可以表成 $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}$ 的线性组合，更因 $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}$ 线性无关，所以 $[S]$ 中任一向量都唯一地表成 $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}$ 的线性组合. 这就是说，$\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}$ 是 $[S]$ 的一组基. 因此 $\dim[S]=|S_0|$.

系理 1 设 V 是域 F 上的一个向量空间，而 S 是 V 的一个有限子集，那么 S 的任意两个极大线性无关子集都含同样个数的元素.

基于这个系理，我们可以给出下面的定义.

定义 1 设 V 是域 F 上的一个向量空间，而 S 是 V 的一个有限子集，S 的任意一个极大线性无关子集中元素的个数就叫做 S 的秩，记作 $\operatorname{rank} S$.

我们有

系理 2 设 V 是域 F 上的一个向量空间，$\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m$ 是 V 中 m 个向量，那么

i) 对任意 i 和 F 中任意一个非零元素 c，都有 $\operatorname{rank}\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}=\operatorname{rank}\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{i-1}, c\mathbf{v}_i, \mathbf{v}_{i+1}, \cdots, \mathbf{v}_m\}$.

ii) 对任意一对 (i, j)，$1\leqslant i<j\leqslant m$，都有 $\operatorname{rank}\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}=\operatorname{rank}\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{i-1}, \mathbf{v}_j, \mathbf{v}_{i+1}, \cdots, \mathbf{v}_{j-1}, \mathbf{v}_i, \mathbf{v}_{j+1}, \cdots, \mathbf{v}_m\}$.

iii) 对任意一对 (i, j)，$1\leqslant i, j\leqslant m$ 而 $i\neq j$，和任意 $d\in F$，都有 $\operatorname{rank}\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}=\operatorname{rank}\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{j-1}, \mathbf{v}_j+d\mathbf{v}_i, \mathbf{v}_{j+1}, \cdots, \mathbf{v}_m\}$.

证. 这是因为

$$[\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m] = [\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{i-1}, c\mathbf{v}_i, \mathbf{v}_{i+1}, \cdots, \mathbf{v}_m]$$
$$= [\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{i-1}, \mathbf{v}_j, \mathbf{v}_{i+1}, \cdots, \mathbf{v}_{j-1}, \mathbf{v}_i, \mathbf{v}_{j+1}, \cdots, \mathbf{v}_m]$$
$$= [\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{j-1}, \mathbf{v}_j + d\mathbf{v}_i, \mathbf{v}_{j+1}, \cdots, \mathbf{v}_m].$$

定义 2 设 V 是 F 上的向量空间，而 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m$ 是 V 中 m 个向量，将向量集合 $S=\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}$ 变成下列向量集之一：

i) $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{i-1}, c\mathbf{v}_i, \mathbf{v}_{i+1}, \cdots, \mathbf{v}_m\}$，其中 c 是 F 中的任意一个 $\neq 0$ 的元素，

ii) $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{i-1}, \mathbf{v}_j, \mathbf{v}_{i+1}, \cdots, \mathbf{v}_{j-1}, \mathbf{v}_i, \mathbf{v}_{j+1}, \cdots, \mathbf{v}_m\}$，其中 $1 \leqslant i < j \leqslant m$，

iii) $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{j-1}, \mathbf{v}_j + d\mathbf{v}_i, \mathbf{v}_{j+1}, \cdots, \mathbf{v}_m\}$，其中 $i \neq j$ 而 $d \in F$，

分别叫做将向量集合 S 进行了第一种．第二种或第三种*初等变换*．第一种初等变换又叫做将 S 中的 $\mathbf{v}_i$ 乘以 F 中一个非零元素 c 的变换，第二种初等变换又叫做将 S 中两个向量 $\mathbf{v}_i$, $\mathbf{v}_j$ 对调位置的初等变换，而第三种初等变换又叫做将 $\mathbf{v}_i$ 乘以 F 中的元素 d 加到 $\mathbf{v}_j$ 上去的初等变换.

这样上面的系理 2 可以改述成

定理 2 设 V 是域 F 上的一个向量空间，而 $S=\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}$ 是 V 的一个有限子集，那么 S 经过初等变换之后并不改变它的秩.

以下设 V 是域 F 上的 n 维向量空间，而 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ 是它的一组基，仍设 $S=\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}$ 是 V 的一个有限子集，那么每个 $\mathbf{v}_i$ 都可以表成 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 的线性组合

$$\mathbf{v}_i = \sum_{j=1}^{n} a_{ij}\mathbf{e}_j, \quad a_{ij} \in F, \quad i=1, 2, \cdots, m. \tag{1}$$

我们可以把 F 中的 mn 个元素 $a_{ij}(i=1, 2, \cdots, m;\ j=1,$

$2, \cdots, n$)排成一个长方形

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

把它叫做域 F 上的 m 行 n 列的矩阵，或 $m\times n$ 矩阵. 我们往往用大写英文字母来代表矩阵. 现在我们把上面矩阵用 A 来代表，有时也把 A 简记作

$$A=(a_{ij})_{1\leq i\leq m, 1\leq j\leq n}.$$

矩阵 A 一共有 m 个行:

$$(a_{11}, a_{12}, \cdots, a_{1n}), (a_{21}, a_{22}, \cdots, a_{2n}),$$
$$\cdots, (a_{m1}, a_{m2}, \cdots, a_{mn});$$

我们把它们叫做 A 的 m 个行向量，并依序叫做 A 的第一个行向量，第二个行向量，…，第 m 个行向量；它们都是 $V_n(F)$ 中的向量. 因此 $V_n(F)$ 又叫 F 上的 n 维行向量空间. 矩阵 A 一共有 n 个列

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix}, \cdots, \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix};$$

我们把它们叫做 A 的 n 个列向量，并依序叫做 A 的第一个列向量，第二个列向量，…，第 n 个列向量. 我们还把 a_{ij} 叫做 A 的第 i 行第 j 列的元素，或叫做 (i, j) 位置的元素.

引理 1 设 $c_1, c_2, \cdots, c_m$ 是 F 中的 m 个元素，那么 $c_1\mathbf{v}_1+c_2\mathbf{v}_2+\cdots+c_m\mathbf{v}_m=\mathbf{0}$，当且仅当

$$c_1(a_{11}, a_{12}, \cdots, a_{1n})+c_2(a_{21}, a_{22}, \cdots, a_{2n})$$
$$+\cdots+c_m(a_{m1}, a_{m2}, \cdots, a_{mn})=\underbrace{(0, 0, \cdots, 0)}_{n\text{个}} \qquad (2)$$

证. 设

$$\sum_{i=1}^{m} c_i \mathbf{v}_i = \mathbf{0}. \tag{3}$$

将(1)代入上式得

$$\mathbf{0} = \sum_{i=1}^{m} c_i \sum_{j=1}^{n} a_{ij}\mathbf{e}_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} c_i a_{ij}\right) \mathbf{e}_j.$$

因$\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$是$V$的一组基，所以

$$\sum_{i=1}^{m} c_i a_{ij} = 0,\ j = 1,\ 2,\ \cdots,\ n. \tag{4}$$

而(4)中n个式子就是说(2)式右方n维行向量的n个分量都等于0，因此(2)式成立.

反过来，如果(2)式成立，那么(4)式成立. 将(4)式双方乘以$\mathbf{e}_j$，再对$j(=1, 2, \cdots, m)$求和，然后利用(1)式就可推出(3)式成立.

从引理1立刻推出

定理3 设V是F中的n维向量空间，而$\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$是它的一组基，再设$S = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}$是$V$的一个有限子集. 将每个$\mathbf{v}_i$都表成$\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$的线性组合

$$\mathbf{v}_i = \sum_{j=1}^{n} a_{ij}\mathbf{e}_j,\ a_{ij} \in F,\ i = 1,\ 2,\ \cdots,\ m.$$

令
$$A = (a_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}.$$

那么S的秩就等于A的m个行向量组成的集合的秩.

证. 从引理1显然可推出：如果$\{\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_r}\}$ $(1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant m)$是$S$的一个极大线性无关向量组，那么$A$的第$i_1$行，第$i_2$行，$\cdots$，第$i_r$行就是$A$的$m$个行向量组成的集合的一个极大线性无关向量组；而且反过来也对. 因此S的秩就等于A的m个行向量组成的集合的秩.

这样一来，研究一个$m \times n$矩阵的m个行向量组成的集合的秩是有意义的. 我们有

定义 3 设 A 是域 F 上的一个 $m\times n$ 矩阵. 我们把 A 的 m 个行向量组成的集合的秩叫做矩阵 A 的秩. 换句话说, 矩阵 A 的秩就是它的一个极大线性无关行向量组中向量的个数. 我们把矩阵 A 的秩记作 $\operatorname{rank} A$.

设 A 是域 F 上的 $m\times n$ 矩阵, 那么 A 一共有 m 个行向量. 因此 A 的一个极大线性无关行向量组中的元素个数一定 $\leqslant m$, 这就是说

$$\operatorname{rank} A\leqslant m.$$

另一方面, A 的行向量都是 $V_n(F)$ 中的向量, 而 $\dim V_n(F)=n$, 所以又有

$$\operatorname{rank} A\leqslant n.$$

因此
$$\operatorname{rank} A\leqslant\min(m, n),$$
这里 $\min(m, n)$ 表示 m 和 n 这两个数的极小值.

为了研究矩阵的秩, 根据定理 2, 我们可以对它的行向量组成的集合进行初等变换, 这样并不改变它的秩.

定义 4 设 A 是域 F 上的一个 $m\times n$ 矩阵. 我们把下面这三种变换叫做作用在矩阵 A 的行上的初等变换; 它们是

i) 把 A 的任一行乘以 F 中的一个非零元素, 而不改变 A 的其余 $m-1$ 行.

ii) 把 A 的任意两行对调, 而不改变 A 的其余 $m-2$ 行.

iii) 把 A 的某一行加上另外一行乘以 F 中任一元素的乘积, 而不改变其余 $m-1$ 行.

我们还分别把这三种初等变换叫做作用在 A 的行上的第一种. 第二种和第三种初等变换.

从定理 2 和定义 4 立刻推出

定理 4 设 A 是域 F 上的一个 $m\times n$ 矩阵. 作用在 A 的行上的初等变换并不改变 A 的秩.

因此, 为了计算 A 的秩, 可以对 A 的行连续进行有限次

初等变换，将 A 化成尽可能简单的形状.

定义 5 设 A 是域 F 上的一个 $m\times n$ 矩阵. 如果对 A 的行连续进行有限次初等变换将 A 变成 B, 我们就说 A 与 B 行等价.

注意，作用在一个矩阵的行上的初等变换是可逆的，这就是说，将 A 的第 i 行乘以 F 中一个非零元素 c 把 A 变成 A_1, 那么将 A_1 的第 i 行乘以 c^{-1} 就把 A_1 变成 A; 将 A 的第 i 行和第 j 行 $(i\neq j)$ 对调得到 A_1, 那么将 A_1 的第 i 行和第 j 行对调就得到 A; 将 A 的第 j 行加上第 i 行 $(i\neq j)$ 乘以 F 中的元素 d 的乘积把 A 变成 A_1, 那么将 A_1 的第 j 行加上第 i 行乘以 $-d$ 的乘积就把 A_1 变成 A. 因此如果 A 与 B 行等价，那么 B 也与 A 行等价. 根据定理 4 我们知道行等价的矩阵有相同的秩. 更进一步，我们有下面这个重要的结论.

定理 5 设 A 是域 F 上的一个 $m\times n$ 矩阵，那么 A 一定行等价于以下形状的一个矩阵:

$$A_0=\begin{pmatrix}0\cdots0 & 1 & *\cdots* & 0 & *\cdots* & 0 & *\cdots* & \cdots0 & *\cdots*\\ 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & 0 & *\cdots* & \cdots0 & *\cdots*\\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & \cdots0 & *\cdots*\\ \cdots & & \cdots & & \cdots & & \cdots & \cdots & \cdots\\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & \cdots1 & *\cdots*\\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & \cdots0 & 0\cdots0\\ \cdots & & \cdots & & \cdots & & \cdots & \cdots & \cdots\\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & \cdots0 & 0\cdots0\end{pmatrix}\tag{5}$$

其中 * 表示 F 中的某个元素. 更进一步，设 $\operatorname{rank} A=r$, 那么 A_0 的第 r 行下面的元素都是 0, A_0 的前 r 行中从左往右数第一个非零元素都是 1, 这 r 个 1 分属于 r 个不同的列; 这每一个 1 的同行左侧的元素都是 0, 同列的其他元素也都是 0, 它左下方的元素也都是 0. 因此如果 A_0 的第 i 行 $(1\leqslant i\leqslant r)$

的第一个不等于0的元素1位于第k_i列，那么$1\leqslant k_1<k_2<\cdots<k_r\leqslant n$. （我们把形如$A_0$的矩阵叫做阶梯形矩阵）.

证. 记 $$A=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}.$$

先考察A的第1列. 分两种情形.

1) 如果A的第1列的元素全都是0，就去考察A的第2列.

2) 设A的第1列中有不等于0的元素，依序进行以下步骤：

2.1) 如果$a_{i1}\neq 0$，而$i>1$，就将A的第1行与第i行对调. 将所得矩阵仍记作A. 如果$i=1$，就不做这一步.

2.2) 用a_{11}^{-1}去乘A的第1行，将所得矩阵仍记作A，那么$a_{11}=1$. 如果原来就有$a_{11}=1$，譬如$F=\mathbf{F}_2$时，就不做这一步.

2.3) 将A的第1行乘以$-a_{21}$加到第2行上去，乘以$-a_{31}$加到第3行去，……，乘以$-a_{m1}$加去第m行上去. 把这样得到的矩阵仍记作A. 那么A的第1列中除$(1,1)$位置元素是1以外，其余元素都是0. 然后去考察A的第2列.

现在去考察A的第2列. 分成下面三种情况：

1) 如果A的第1列的元素都是0，那么就象上面考察并处理A的第1列一样来考察并处理A的第2列. 将所得矩阵仍记作A. 再去考察A的第3列.

2) 如果A的第1列的元素除$a_{11}=1$以外其余元素都是0，而A的第2列中除a_{21}可以是F中任意元素外其余元素都是0，那么就去考察A的第3列.

3) 设A的第1列的元素除$a_{11}=1$以外其余元素都是0，而A的第2列中$(2, 2)$, $(3,2)$, ……, $(m, 2)$位置的元素有不等于0的. 依序进行以下步骤：

3.1) 如果 $a_{i2}\neq 0$, 而 $i>2$, 就将 A 的第 2 行与第 i 行对调, 将所得矩阵仍记作 A. 如果 $i=2$, 就不做这一步.

3.2) 用 a_{22}^{-1} 去乘 A 的第 2 行, 将所得矩阵仍记作 A. 如果原来就有 $a_{22}=1$, 譬如 $F=\mathbf{F}_2$ 时, 就不做这一步.

3.3) 将 A 的第 2 行乘以 $-a_{12}$ 加到第 1 行去, 乘以 $-a_{23}$ 加到第 3 行去, ……, 乘以 $-a_{m2}$ 加到第 m 行去, 把这样得到的矩阵仍记作 A. 那么 A 前 2 列中除了 $a_{11}=a_{22}=1$ 以外其余元素全都等于 0. 然后去考察 A 的第 3 列.

现在去考察 A 的第 3 列. 分成下面四种情况:

1) 如果 A 的第 1 列和第 2 列的元素都是 0, 就象上面考察并处理 A 的第 1 列一样去考察并处理 A 的第 3 列.

2) 如果 A 的第 1 列的元素都是 0, 而第 2 列的元素除 $a_{12}=1$ 以外其余元素都是 0, 或者如果 A 的第 1 列的元素除 $a_{11}=1$ 以外其余元素都是 0, 而第 2 列中 $a_{22}=a_{32}=\cdots=a_{m2}=0$, 那么就象前面考察并处理 A 的第 2 列的情形 2) 或 3) 一样去考察并处理 A 的第 3 列.

3) 如果 A 的第 1 列和第 2 列中除了 $a_{11}=a_{22}=1$ 以外其余元素都是 0, 而 A 的第 3 列中 $(3, 3)$, $(4, 3)$, $\cdots$, $(m, 3)$ 位置的元素也都是 0, 那么就去考察 A 的第 4 列.

4) 设 A 的第 1 列和第 2 列中除了 $a_{11}=a_{22}=1$ 以外其余元素都是 0, 而 A 的第 3 列中 a_{33}, a_{43}, $\cdots$, a_{m3} 中有不等于 0 的, 依序进行以下步骤:

4.1) 如果 $a_{i3}\neq 0$ 而 $i>3$, 就将 A 的第 3 行和第 i 行对调. 将所得矩阵仍记作 A. 如果 $i=3$, 就不做这一步.

4.2) 将 A 的第 3 行乘以 a_{33}^{-1}. 把所得矩阵仍记作 A, 那么 $a_{33}=1$. 如果原来就有 $a_{33}=1$, 譬如 $F=\mathbf{F}_2$ 时, 就不做这一步.

4.3) 将 A 的第 3 行乘以 $-a_{13}$ 加到第 1 行上去，乘以 $-a_{23}$ 加到第 2 行上去，乘以 $-a_{43}$ 加到第 4 行上去，……，乘以 $-a_{m3}$ 加到第 m 行上去．把这样得到的矩阵仍记作 A．那么 A 的第 3 列中除 $(3, 3)$ 位置元素是 1 以外，其余元素都是 0．再去考察 A 的第 4 列．

如此继续下去，就可以将 A 经有限次行的初等变换化成 A_0．显然如果 A_0 的前 r 行中有不等于 0 的元素，而第 r 行后面的元素全都是 0，那么 A_0 的前 r 行中第一个等于 1 的元素属于 r 个不同的列，因此 A_0 的前 r 行线性无关，于是 A_0 的秩就是 r．

这样定理 5 就完全证明了．

要计算一个矩阵的秩，对它的行进行有限次初等变换，将它化成阶梯形矩阵后，它的秩立刻就看出来了．而定理 5 的证明方法实际上给出了一个将矩阵化成阶梯形矩阵的方法，这个方法就叫做消去法，我们举一个例子来阐明这个算法．

例 将 $\mathbf{F}_2$ 上的 8×8 矩阵

$$B=\begin{pmatrix} 0&0&0&0&1&0&1&1\\ 0&1&0&0&1&0&1&0\\ 0&1&1&0&1&1&1&1\\ 0&0&0&1&1&1&1&1\\ 0&0&1&0&0&1&0&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&1&0&1&0&0\\ 0&0&0&0&0&0&1&0 \end{pmatrix}$$

化成阶梯形矩阵并计算 $\operatorname{rank} B$．

我们用符号“$B\to B_1$”表示用行的初等变换将 B 化成 B_1，

那么我们有

$$\begin{pmatrix}0&0&0&0&1&0&1&1\\0&1&0&0&1&0&1&0\\0&1&1&0&1&1&1&1\\0&0&0&1&1&1&1&1\\0&0&1&0&0&1&0&1\\0&0&0&0&0&0&1&0\\0&0&0&1&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}\to\begin{pmatrix}0&1&0&0&1&0&1&0\\0&0&0&0&1&0&1&1\\0&1&1&0&1&1&1&1\\0&0&0&1&1&1&1&1\\0&0&1&0&0&1&0&1\\0&0&0&0&0&0&1&0\\0&0&0&1&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}$$

$$\to\begin{pmatrix}0&1&0&0&1&0&1&0\\0&0&0&0&1&0&1&1\\0&0&1&0&0&1&0&1\\0&0&0&1&1&1&1&1\\0&0&1&0&0&1&0&1\\0&0&0&0&0&0&1&0\\0&0&0&1&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}\to\begin{pmatrix}0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\\0&0&0&0&1&0&1&1\\0&0&0&1&1&1&1&1\\0&0&1&0&0&1&0&1\\0&0&0&0&0&0&1&0\\0&0&0&1&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}$$

$$\to\begin{pmatrix}0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\\0&0&0&0&1&0&1&1\\0&0&0&1&1&1&1&1\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&1&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}\to\begin{pmatrix}0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\\0&0&0&1&1&1&1&1\\0&0&0&0&1&0&1&1\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&1&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}$$

$$\to\begin{pmatrix}0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\\0&0&0&1&1&1&1&1\\0&0&0&0&1&0&1&1\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&1&0&1&1\\0&0&0&0&0&0&1&0\end{pmatrix}\to\begin{pmatrix}0&1&0&0&0&0&0&1\\0&0&1&0&0&1&0&1\\0&0&0&1&0&1&0&0\\0&0&0&0&1&0&1&1\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}$$

$$\to\begin{pmatrix}0&1&0&0&0&0&0&1\\0&0&1&0&0&1&0&1\\0&0&0&1&0&1&0&0\\0&0&0&0&1&0&1&1\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}\to\begin{pmatrix}0&1&0&0&0&0&0&1\\0&0&1&0&0&1&0&1\\0&0&0&1&0&1&0&0\\0&0&0&0&1&0&0&1\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{pmatrix}$$

因此 $\operatorname{rank} B=5$.

在定义 3 里，我们定义的矩阵的秩是对矩阵的行来说的．平行地，我们考察域 $\mathbf{F}$ 上的 n 维列向量

$$\begin{pmatrix}v_1\\v_2\\\vdots\\v_m\end{pmatrix},\ v_i\in F$$

的全体所组成的 F 上的m维列向量空间，并把 F 上的 $m\times n$ 矩阵 A 的 n 个列看作 F 上m维列向量空间中的向量．我们有

定义 6 设 A 是域 F 上的一个 $m\times n$ 矩阵．我们把 A

的 n 个列向量组成的集合的秩叫做矩阵 A 的列秩. 换句话说，矩阵 A 的列秩就是它的一个极大线性无关列向量组中向量的个数.

我们也可以平行于定义 4 来定义作用在矩阵 A 的列上的初等变换，并平行于定理 4 去证明作用在 A 的列上的初等变换并不改变 A 的列秩. 但重要的是，我们还有

定理 6 设 A 是域 F 上的一个 $m\times n$ 矩阵，那么作用在 A 的行上的初等变换并不改变 A 的列秩.

证. 先设将 A 的第 i 行乘上 F 中的一个非零元素 c，得到 A_1. 我们来证明 A 的列秩等于 A_1 的列秩. 写

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

那么

$$A_1=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ ca_{i1} & ca_{i2} & \cdots & ca_{in} \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

设 A 的列秩等于 r，并假定 A 的第 $j_1, j_2, \cdots, j_r$ 列组成 A 的一个极大线性无关列向量组. 我们来证明 A_1 的第 $j_1, j_2, \cdots, j_r$ 列线性无关. 设有线性关系

$$c_1\begin{pmatrix} a_{1j_1} \\ \vdots \\ ca_{ij_1} \\ \vdots \\ a_{mj_1} \end{pmatrix}+c_2\begin{pmatrix} a_{1j_2} \\ \vdots \\ ca_{ij_2} \\ \vdots \\ a_{mj_2} \end{pmatrix}+\cdots+c_r\begin{pmatrix} a_{1j_r} \\ \vdots \\ ca_{ij_r} \\ \vdots \\ a_{mj_r} \end{pmatrix}=\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ c_i\in F,$$

那么

$$\left.\begin{array}{l}c_1a_{1j_1}+c_2a_{1j_2}+\cdots+c_ra_{1j_r}=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ c_1ca_{ij_1}+c_2ca_{ij_2}+\cdots+c_rca_{ij_r}=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ c_1a_{mj_1}+c_2a_{mj_2}+\cdots+c_ra_{mj_r}=0,\end{array}\right\}$$

由于 $c\neq0$，将上面 m 个式子中的第 i 个乘以 c^{-1} 就得到

$$c_1a_{ij_1}+c_2a_{ij_2}+\cdots+c_ra_{ij_r}=0.$$

因此

$$c_1\begin{pmatrix}a_{1j_1}\\ \vdots\\ a_{ij_1}\\ \vdots\\ a_{mj_1}\end{pmatrix}+c_2\begin{pmatrix}a_{1j_2}\\ \vdots\\ a_{ij_2}\\ \vdots\\ a_{mj_2}\end{pmatrix}+\cdots+c_r\begin{pmatrix}a_{1j_r}\\ \vdots\\ a_{ij_r}\\ \vdots\\ a_{mj_r}\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

但 A 的第 $j_1, j_2, \cdots, j_r$ 列线性无关，所以 $c_1=c_2=\cdots=c_r=0$. 这证明了 A_1 的第 $j_1, j_2, \cdots, j_r$ 列线性无关. 由此推出 A_1 的列秩大于或等于 A 的列秩 r. 反过来，将 A_1 的第 i 行乘以 c^{-1} 就得到 A. 因此，同理可证 A 的列秩 r 大于或等于 A_1 的列秩，所以 A_1 的列秩等于 A 的列秩.

作用在 A 的行上的第二种初等变换不改变 A 的列秩是很显然的，我们就不把证明写出来了.

现在设将 A 的第 j 行加上第 i 行乘以 F 中任一元素 d

的乘积之后得到 A_1，那么

$$A_1=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{j1}+da_{i1} & a_{j2}+da_{i2} & \cdots & a_{jn}+da_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

仍设 A 的列秩等于 r，并假定 A 的第 j_1, j_2, $\cdots$, j_r 列组成 A 的一个极大线性无关列向量组，我们来证明 A_1 的第 j_1, j_2, $\cdots$, j_r 列也线性无关．设有线性关系

$$c_1\begin{pmatrix} a_{1j_1} \\ \vdots \\ a_{ij_1} \\ \vdots \\ a_{jj_1}+da_{ij_1} \\ \vdots \\ a_{mj_1} \end{pmatrix}+c_2\begin{pmatrix} a_{1j_2} \\ \vdots \\ a_{ij_2} \\ \vdots \\ a_{jj_2}+da_{ij_2} \\ \vdots \\ a_{mj_2} \end{pmatrix}$$

$$+\cdots+c_r\begin{pmatrix} a_{1j_r} \\ \vdots \\ a_{ij_r} \\ \vdots \\ a_{jj_r}+da_{ij_r} \\ \vdots \\ a_{mj_r} \end{pmatrix}=\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ c_i\in F,$$

那么

$$\left.\begin{array}{l}c_1a_{1j_1}+c_2a_{1j_2}+\cdots+c_ra_{1j_r}=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ c_1a_{ij_1}+c_2a_{ij_2}+\cdots+c_ra_{ij_r}=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ c_1(a_{jj_1}+da_{ij_1})+c_2(a_{jj2}+da_{ij_2})+\cdots+c_r(a_{jj_r}+da_{ij_r})=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ c_1a_{mj_1}+c_2a_{mj_2}+\cdots+c_ra_{mj_r}=0,\end{array}\right\}$$

将上面式子里的第 j 个式子减去第 i 个式子乘以 $-d$ 就得到

$$c_1a_{jj_1}+c_2a_{jj_2}+\cdots+c_ra_{jj_r}=0.$$

因此

$$c_1\begin{pmatrix}a_{1j_1}\\ \vdots\\ a_{ij_1}\\ \vdots\\ a_{jj_1}\\ \vdots\\ a_{mj_1}\end{pmatrix}+c_2\begin{pmatrix}a_{1j_2}\\ \vdots\\ a_{ij_2}\\ \vdots\\ a_{jj_2}\\ \vdots\\ a_{mj_2}\end{pmatrix}+\cdots+c_r\begin{pmatrix}a_{1j_r}\\ \vdots\\ a_{ij_r}\\ \vdots\\ a_{jj_r}\\ \vdots\\ a_{mj_r}\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\\ \vdots\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

但 A 的第 $j_1, j_2, \cdots, j_r$ 列线性无关，所以 $c_1=c_2=\cdots=c_r=0$. 这证明了 A_1 的第 $j_1, j_2, \cdots, j_r$ 列线性无关，由此推出 A_1 的列秩大于或等于 A 的列秩 r. 反过来，将 A_1 的第 j 列加上第 i 列乘以 $-d$ 的乘积就得到 A. 因此同理可证 A 的列秩 r 大于或等于 A_1 的列秩. 所以 A_1 的列秩等于 A 的列秩.

这样定理 6 就完全证明了.

从定理 5 和定理 6 可以推出

定理 7 设 A 是域 F 上的任意一个 $m\times n$ 矩阵，那么 A 的秩一定等于 A 的列秩.

证. 设 A 的秩是 r. 根据定理 5，对 A 的行连续进行有限次初等变换，可将 A 化成阶梯形矩阵 (5)，即定理 5 中的

A_0，而 A_0 的第 r 行后面的元素都是 0，A_0 的第1，2，…，r 行中从左往右数第一个非零元素都是 1，它们分别位于 A_0 的第 k_1，k_2，…，k_r 列，$1\leqslant k_1<k_2<\cdots<k_r\leqslant n$. 显然 A_0 的第 k_1，k_2，…，k_r 列是 A_0 的一个极大线性无关列向量组. 因此 A_0 的列秩等于 r. 但根据定理 6，A 的列秩等于 A_0 的列秩，所以 A 的列秩也等于 r.

基于定理 7，我们把域 F 上矩阵 A 的列秩也叫做它的秩，这并不会引起混淆.

§3 矩阵的运算和线性变换的定义

我们先来引进矩阵的运算. 设

$$A=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n},\quad B=(b_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$$

都是域 F 上的 $m\times n$ 矩阵. 造一个 $m\times n$ 矩阵

$$C=(c_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n},$$

其中

$$c_{ij}=a_{ij}+b_{ij},\ i=1,\ 2,\ \cdots,\ m;\quad j=1,\ 2,\ \cdots,\ n.$$

我们把 C 叫做 A 与 B 的**和**，记作

$$C=A+B.$$

注意，仅当两个矩阵有相同的行数和列数时，才可以相加，即求它们的和.

容易验证，域 F 上所有 $m\times n$ 矩阵对于上面规定的矩阵的加法来说是一个交换群. 特别，我们有

$$A+B=B+A,$$

$$(A+B)+C=A+(B+C).$$

这个交换群的单位元素是所有位置的元素都等于 0 的矩阵，我们把它叫做**零矩阵**，记作 $0^{(m,n)}$，或简记作 0. 而矩阵 $A=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$ 的负元素是 $-A=(-a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$. 当然也

可以引进矩阵的减法

$$A-B=A+(-B),$$

其中 A 和 B 都是 $m\times n$ 矩阵.

再设 A 是 F 上的 $m\times n$ 矩阵, B 是 $n\times l$ 矩阵. 写

$$A=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n},\quad B=(b_{ij})_{1\leqslant i\leqslant n,1\leqslant j\leqslant l},$$

造一个 $m\times l$ 矩阵

$$C=(c_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant l}$$

其中

$$c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj},\quad i=1,\ 2,\ \cdots,\ m;\ j=1,\ 2,\ \cdots,\ l$$

我们把 C 叫做 A 与 B 的积,记作

$$C=AB.$$

注意, 仅当前一个矩阵的列数等于后一个矩阵的行数时两个矩阵才能相乘, 即求它们的积. 两个矩阵相乘可按照“行乘列”的规则进行,即将前一个矩阵第 i 行的元素分别和后一个矩阵第 j 列的相应位置的元素相乘, 然后将所得的 n 个积相加, 这样就得到乘积中的 $(i,\ j)$ 位置的元素. 例如, $\mathbf{F}_2$ 上的矩阵

$$A=\begin{pmatrix}1&0&0&1\\1&1&0&1\end{pmatrix}\quad 与\quad B=\begin{pmatrix}1&0&1\\0&1&0\\1&0&0\\0&1&1\end{pmatrix}$$

的乘积是

$$AB=\begin{pmatrix}1\cdot1+0\cdot0+0\cdot1+1\cdot0 & 1\cdot0+0\cdot1+0\cdot0+1\cdot1 & 1\cdot1+0\cdot0+0\cdot0+1\cdot1\\ 1\cdot1+1\cdot0+0\cdot1+1\cdot0 & 1\cdot0+1\cdot1+0\cdot0+1\cdot1 & 1\cdot1+1\cdot0+0\cdot0+1\cdot1\end{pmatrix}$$

$$=\begin{pmatrix}1&1&0\\1&0&0\end{pmatrix}$$

容易验证，矩阵乘法是结合的，而且对于加法是分配的；即

$$(AB)C=A(BC),$$
$$A(B+C)=AB+AC,$$
$$(A+B)C=AC+AC,$$

只要上面这些式子里出现的矩阵相乘和相加都有定义．即使当 A 和 B 都是 $n\times n$ 矩阵时，也可能有 $AB\neq BA$．例如，考察 $\mathbf{F}_2$ 上的矩阵

$$A=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix},\ B=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}.$$

我们有
$$AB=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},\ BA=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}.$$

设 A 是 $n\times n$ 矩阵，我们把 A 的 $(1, 1)$，$(2, 2)$，$\cdots$，(n, n) 位置叫做 A 的主对角线，如果 A 的主对角线以外的元素都等于 0，A 就叫做对角矩阵．如果 A 的主对角线以下位置的元素都等于 0，A 就叫做上三角形矩阵．如果 A 的主对角线以上位置的元素都等于 0，A 就叫做下三角形矩阵．我们用 $I^{(n)}$ 来代表主对角线上的元素都等于 1 的 $n\times n$ 对角矩阵，并把它叫做 $n\times n$ 单位矩阵．有时我们也把 $I^{(n)}$ 简记作 I．显然对任意 $m\times n$ 矩阵 A，有

$$AI^{(n)}=A,\ I^{(m)}A=A.$$

设 A 是域 F 上的一个 $n\times n$ 矩阵．如果域 F 上有一个 $n\times n$ 矩阵 B 适合条件

$$AB=BA=I,$$

A 就叫可逆矩阵，而 B 叫 A 的一个逆矩阵．如果 B_1 是 A 的另一个逆矩阵，即

$$AB_1=B_1A=I,$$

那么
$$B=BI=B(AB_1)=(BA)B_1=IB_1=B_1.$$

因此可逆矩阵的逆矩阵是唯一确定的. 我们把可逆矩阵 A 的逆矩阵记作 A^{-1}. 显然 A^{-1} 也是可逆矩阵, 而

$$(A^{-1})^{-1}=A.$$

又如果 A, B 都是 $n\times n$ 可逆矩阵, 那么 AB 也是可逆矩阵, 而

$$(AB)^{-1}=B^{-1}A^{-1}.$$

容易验证, 域 F 上所有 $n\times n$ 可逆矩阵所组成的集合对于矩阵乘法组成一个群. 这个群不是交换群. 它的单位元素就是单位矩阵, 而 A 的逆元素就是 A^{-1}. 例如, $\mathbf{F}_2$ 上一共有下面 6 个 2×2 可逆矩阵

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}0&1\\1&0\end{pmatrix},\ \begin{pmatrix}1&1\\0&1\end{pmatrix},$$

$$\begin{pmatrix}1&0\\1&1\end{pmatrix},\ \begin{pmatrix}1&1\\1&0\end{pmatrix},\ \begin{pmatrix}0&1\\1&1\end{pmatrix}.$$

它们组成一个 6 阶群.

下面的定理说明了可逆矩阵的一个几何意义.

定理 1 设 V 是域 F 上的 n 维向量空间, $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ 是它的一组基. 设 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ 是 V 中 n 个向量, 将 $\mathbf{v}_i(1\leqslant i\leqslant n)$ 表成 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 的线性组合:

$$\mathbf{v}_i=\sum_{j=1}^{n}a_{ij}\mathbf{e}_j,\ a_{ij}\in F,\ i=1, 2, \cdots, n. \tag{1}$$

令

$$A=(a_{ij})_{1\leqslant i, j\leqslant n}.$$

那么 A 是可逆矩阵, 当且仅当 $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$ 也是 V 的一组基.

证. 设 A 是可逆矩阵, 即有 $n\times n$ 矩阵 B 使

$$AB=BA=I.$$

将 B 写作

$$B=(b_{ij})_{1\leqslant i, j\leqslant n},$$

那么

$$\sum_{j=1}^{n} b_{ij}a_{jk}=\begin{cases}1, & \text{如果 } i=k,\\ 0, & \text{如果 } i\neq k.\end{cases} \tag{2}$$

将(1)式中 i 改作 j, j 改作 k, 就有

$$\mathbf{v}_j=\sum_{k=1}^{n} a_{jk}\mathbf{e}_k.$$

将上式双方乘以 b_{ij}, 再向 j 求和, 然后利用(2)式, 就得到

$$\sum_{j=1}^{n} b_{ij}\mathbf{v}_j=\sum_{j=1}^{n} b_{ij}\sum_{k=1}^{n} a_{jk}\mathbf{e}_k=\sum_{k=1}^{n}\left(\sum_{j=1}^{n} b_{ij}a_{jk}\right)\mathbf{e}_k=\mathbf{e}_i.$$

这是说 $\mathbf{e}_i(1\leqslant i\leqslant n)$ 表成了 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ 的线性组合. 因 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$是 V 的一组基, 所以 V 的任一向量都可以表成 $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ 的线性组合, 那么$\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$ 的一个极大线性无关向量组就是 V 的一组基. 因 $\dim V=n$, V 的任意一组基中元素个数都是 n, 所以$\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$ 就是 V 的一组基.

反过来, 设$\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$是 V 的一组基, 那么有

$$\mathbf{e}_i=\sum_{j=1}^{n} b_{ij}\mathbf{v}_j,\ b_{ij}\in F,\ i=1, 2, \cdots, n. \tag{3}$$

将(3)式中 i 改成 j, j 改成 k, 再代入(1)式, 就得到

$$\mathbf{v}_i=\sum_{j=1}^{n} a_{ij}\sum_{k=1}^{n} b_{jk}\mathbf{v}_k=\sum_{k=1}^{n}\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)\mathbf{v}_k.$$

因$\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$是 V 的一组基, 所以

$$\sum_{j=1}^{n} a_{ij}b_{jk}=\begin{cases}1, & \text{如果 } i=k,\\ 0, & \text{如果 } i\neq k.\end{cases} \tag{4}$$

令

$$B=(b_{ij})_{1\leqslant i,j\leqslant n},$$

那么(4)式就是说

$$AB=I. \tag{5}$$

另一方面, 将(1)式中的 i 改成 j, j 改成 k, 再代入(3)式, 就得到

$$e_i=\sum_{j=1}^{n}b_{ij}\sum_{k=1}^{n}a_{jk}e_k=\sum_{k=1}^{n}\left(\sum_{j=1}^{n}b_{ij}a_{jk}\right)e_k.$$

因$\{e_1, e_2, \cdots, e_n\}$是$V$的一组基，所以

$$\sum_{j=1}^{n}b_{ij}a_{jk}=\begin{cases}1, & \text{如果 } i=k,\\ 0, & \text{如果 } i\neq k.\end{cases}$$

这就是说

$$BA=I. \tag{6}$$

由(5)，(6)两式可知A是可逆矩阵.

这证明了定理1.

仍设A是域F上的一个$n\times n$矩阵，而$m\geqslant 1$. 规定

$$A^m=\underbrace{A\cdot A\cdot\cdots\cdot A}_{m\text{个}}.$$

容易验证，当$m, n\geqslant 1$时，有

$$A^m\cdot A^n=A^{m+n}, \tag{7}$$

$$(A^m)^n=A^{mn}. \tag{8}$$

当A是可逆矩阵时，还可以定义

$$A^0=I,$$

$$A^{-m}=(A^{-1})^m, \quad m\geqslant 1.$$

这时，(7)，(8)两式对于任意整数m和n都成立.

再设A是域F上的一个$m\times n$矩阵，写

$$A=(a_{ij})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$$

设$c\in F$. 造一个矩阵

$$C=(c_{ij})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n},$$

其中 $c_{ij}=ca_{ij}, \ i=1, 2, \cdots, m; \ j=1, 2, \cdots, n.$

我们把C叫做用F中的元素c去乘A所得的积，记作

$$C=cA.$$

容易验证，F上所有$m\times n$矩阵组成的集合对于矩阵加

法和用 F 中元素去乘矩阵的乘法来说，是一个向量空间．特别，我们有

$$c(A+B)=cA+cB,$$
$$(c+d)A=cA+dA,$$
$$(cd)A=c(dA),$$
$$1A=A.$$

用 E_{ij} 表示仅在 $(i,\ j)$ 位置上的元素是 1，而其余位置上的元素都是 0 的 $m\times n$ 矩阵，那么任一 $m\times n$ 矩阵

$$A=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$$

可唯一地表成

$$A=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}E_{ij}.$$

因此 $\{E_{ij}|i=1,\ 2,\ \cdots,\ m;\ j=1,\ 2,\ \cdots,\ n\}$ 是这个向量空间的一组基．还可以验证下面的运算规则也成立：

$$c(AB)=(cA)B=A(cB).$$

把一个矩阵 A 的行列互换，所得到的矩阵叫做 A 的**转置矩阵**，记作 A'．设 A 是 $m\times n$ 矩阵：

$$A=\begin{pmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ a_{m1} & a_{m2} & \cdots & a_{mn}\end{pmatrix},$$

那么 A' 就是 $n\times m$ 矩阵：

$$A'=\begin{pmatrix}a_{11} & a_{21} & \cdots & a_{m1}\\ a_{12} & a_{22} & \cdots & a_{m2}\\ \cdots & \cdots & \cdots & \cdots\\ a_{1n} & a_{2n} & \cdots & a_{mn}\end{pmatrix}.$$

容易验证

$$(A')'=A,$$
$$(A+B)'=A'+B',$$

$$(AB)' = B'A',$$
$$(cA)' = cA'.$$

上面我们引进了矩阵的四种运算，即加法运算，乘法运算，用 F 中的元素去乘矩阵的运算和转置运算，并列出了它们的一些运算规则．这些运算以后常要用到．

我们先利用矩阵的乘法运算去研究矩阵的行的初等变换．我们把下面三种形状的 $m\times m$ 矩阵叫做 $m\times m$ 初等矩阵

$$\text{i)}\quad D_i(c)=\begin{pmatrix}1&&&&&&\\&1&&&&&\\&&\ddots&&&&\\&&&1&&&\\&&&&c&&\\&&&&&1&\\&&&&&&\ddots\\&&&&&&&1\end{pmatrix}\begin{matrix}\\\\\\\\ \text{第 } i \text{ 行}\\\\\\\\\end{matrix}$$
$$\text{(}c\text{ 所在列：第 } i \text{ 列)}$$

这是一个对角矩阵，主对角线上除 (i, i) 位置元素是 c 以外，其余元素都是 1，而 $c\neq 0$．（我们永远约定，矩阵中没有写出元素的空白地方都是一些 0．）

$$\text{ii)}\quad P_{ij}=\begin{pmatrix}1&&&&&&&&\\&\ddots&&&&&&&\\&&1&&&&&&\\&&&0&&&1&&\\&&&&1&&&&\\&&&&&\ddots&&&\\&&&&&&1&&\\&&&1&&&0&&\\&&&&&&&1&\\&&&&&&&&\ddots\\&&&&&&&&&1\end{pmatrix}\begin{matrix}\\\\\\\text{第 } i \text{ 行}\\\\\\\\\text{第 } j \text{ 行}\\\\\\\\\end{matrix}$$
$$\text{(第 } i \text{ 列} \qquad \text{第 } j \text{ 列)}$$

$$
\text{iii) } T_{ij}(d)=\begin{pmatrix}1&&&&&&\\&1&&&&&\\&&\ddots&&&&\\&&&1&&d&\\&&&&\ddots&&\\&&&&&1&\\&&&&&&\ddots\\&&&&&&&1\end{pmatrix}\begin{matrix}\\ \\ \\ \text{第 } i \text{ 行}\\ \\ \text{第 } j \text{ 行}\\ \\ \\ \end{matrix}
$$

第 i 列　第 j 列

不难看出，将一个 $m\times n$ 矩阵 A 从前面乘以 $D_i(c)$ 相当于将 A 的第 i 行乘以 c 而其余 $m-1$ 行都不变的作用在行上的第一种初等变换．将 A 从前面乘以 P_{ij} 相当于将 A 的 i，j 两行对调而不改变其余 $m-2$ 行的第二种初等变换．将 A 从前面乘以 $T_{ij}(d)$ 相当于将 A 的第 i 行加上第 j 行乘以 d 的乘积而不改变其余 $m-1$ 行的第三种初等变换．因此我们把 $D_i(c)$，P_{ij}，$T_{ij}(d)$ 分别称为第一种、第二种和第三种*初等矩阵*．同样，将 $m\times n$ 矩阵 A 从后面乘以 $n\times n$ 初等矩阵 $D_i(c)$，P_{ij} 和 $T_{ij}(d)$ 分别相当于在 A 的列上作用以第一种、第二种和第三种初等变换．

显然初等矩阵都是可逆矩阵，而且它们的逆矩阵仍是初等矩阵．实际上，

$$
\begin{aligned}
D_i(c)^{-1}&=D_i(c^{-1}),\\
P_{ij}^{-1}&=P_{ij},\\
T_{ij}(d)^{-1}&=T_{ij}(-d).
\end{aligned}
$$

引进了初等矩阵以后，§2 定理 5 可以改述成

定理 2　设 A 是域 F 上的 $n\times n$ 矩阵，那么可以将 A 从前面依序乘上有限个初等矩阵以后化成一个阶梯形矩阵．

我们可以利用矩阵的秩来判断一个 $n\times n$ 矩阵是否可逆．我们有

定理3 设 A 是域 F 上的 $n\times n$ 矩阵，那么 A 是可逆矩阵，当且仅当 $\operatorname{rank} A=n$.

证. 设 A 是可逆矩阵，那么有矩阵 B 存在使

$$BA=I. \tag{9}$$

令
$$B=(b_{ij})_{1\leqslant i,j\leqslant n},$$

那么比较(9)式双方第 i 行 $(1\leqslant i\leqslant n)$ 就得到

$$(b_{i1}b_{i2}\cdots b_{in})A=\mathbf{e}_i,\ i=1,\ 2,\ \cdots,\ n, \tag{10}$$

而 $\mathbf{e}_i$ 是第 i 个分量是1而其余分量都是0的 n 维行向量. 将 A 的第 j 行 $(1\leqslant j\leqslant n)$ 的行向量记作 $\mathbf{a}_j$，那么(10)式可写作

$$\sum_{j=1}^{n} b_{ij}\mathbf{a}_j=\mathbf{e}_i,\ i=1,\ 2,\cdots,\ n.$$

这就是说，$\mathbf{e}_1,\ \mathbf{e}_2,\ \cdots,\ \mathbf{e}_n$ 都可以表成 $\mathbf{a}_1,\ \mathbf{a}_2,\ \cdots,\ \mathbf{a}_n$ 的线性组合. 因 $\{\mathbf{e}_1,\ \mathbf{e}_2,\ \cdots,\ \mathbf{e}_n\}$ 是 $V_n(F)$ 的一组基，所以 $V_n(F)$ 中任一向量都可以表成 $\mathbf{a}_1,\ \mathbf{a}_2,\ \cdots,\ \mathbf{a}_n$ 的线性组合. 这样 $\{\mathbf{a}_1,\ \mathbf{a}_2,\ \cdots,\ \mathbf{a}_n\}$ 的一个极大线性无关组就是 $V_n(F)$ 的一组基. 但 $\dim V_n(F)=n$，$V_n(F)$ 的任何一组基都由 n 个向量组成，所以 $\{\mathbf{a}_1,\ \mathbf{a}_2,\ \cdots,\ \mathbf{a}_n\}$ 就是 $V_n(F)$ 的一组基. 因此 $\mathbf{a}_1,\ \mathbf{a}_2,\ \cdots,\ \mathbf{a}_n$ 线性无关. 于是 $\operatorname{rank} A=n$.

反过来，设 $\operatorname{rank} A=n$，那么根据定理2，有有限个初等矩阵 $E_1,\ E_2,\ \cdots,\ E_s$，将它们依序从前面乘 A 以后，得到的矩阵

$$A_0=E_sE_{s-1}\cdots E_2E_1A$$

是阶梯形矩阵. 因 $\operatorname{rank} A=n$，A_0 不能有元素全都是0的行出现，而且 A_0 的 n 行中从左往右数第一个非零元素都是1，这 n 个1分属于 n 个不同的列，它们同列的其它元素都是0. 这就是说 $A_0=I$，即

$$E_sE_{s-1}\cdots E_2E_1A=I. \tag{11}$$

因初等矩阵都是可逆矩阵，所以将上式双方从前面依次乘上

E_s^{-1}, E_{s-1}^{-1}, $\cdots$, E_2^{-1}, E_1^{-1} 之后得出

$$A=E_1^{-1}E_2^{-1}\cdots E_s^{-1}. \tag{12}$$

再将上式双方从后面依次乘上 E_s, E_{s-1}, $\cdots$, E_2, E_1 之后得到

$$AE_sE_{s-1}\cdots E_2E_1=I. \tag{13}$$

(11)、(13)二式表明 A 是可逆矩阵.

这证明了定理 3.

在证明定理 3 的过程中我们实际上还证明了

系理 1 设 A 是域 F 上的 $n\times n$ 可逆矩阵，那么 A 一定是有限个初等矩阵的乘积.

证. 注意，在定理 3 的证明中我们得出了(12)式. 因初等矩阵的逆矩阵仍是初等矩阵，所以 A 是有限个初等矩阵的乘积.

我们还有

系理 2 设 A 和 B 是域 F 上的两个 $m\times n$ 矩阵，那么 A 和 B 行等价，当且仅当有 $m\times m$ 可逆矩阵 P 使 $PA=B$.

证. 设 A 和 B 行等价，那么就有有限个 $m\times m$ 初等矩阵 E_1, E_2, $\cdots$, E_s 存在使

$$E_sE_{s-1}\cdots E_2E_1A=B.$$

令

$$P=E_sE_{s-1}\cdots E_2E_1,$$

就有

$$PA=B.$$

反过来，设 $PA=B$，而 P 是可逆矩阵. 根据系理 1，可将 P 表成有限个初等矩阵 E_1, E_2, $\cdots$, E_s 的乘积

$$P=E_sE_{s-1}\cdots E_2E_1$$

于是

$$E_sE_{s-1}\cdots E_2E_1A=B,$$

这就是说 A 和 B 行等价.

下面我们介绍一下矩阵的分块. 这是一种比较方便的处理矩阵的方法. 先看一个例子. 考察 $\mathbf{F}_2$ 上的 4×4 矩阵

$$A=\begin{pmatrix}1&0&0&0\\0&1&0&0\\1&0&1&1\\1&1&1&0\end{pmatrix}.$$

如果令
$$A_{11}=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad A_{12}=\begin{pmatrix}0&0\\0&0\end{pmatrix},$$
$$A_{21}=\begin{pmatrix}1&0\\1&1\end{pmatrix},\quad A_{22}=\begin{pmatrix}1&1\\1&0\end{pmatrix},$$

就可以将 A 写作
$$A=\begin{pmatrix}A_{11}&A_{12}\\A_{21}&A_{22}\end{pmatrix},$$

这时 A 中的 A_{11}, A_{12}, A_{21}, A_{22} 都是 2×2 矩阵. 一般地, 设 A 是域 F 上的 $m\times n$ 矩阵, 假定 m 可以分成 s 个正整数 m_1, m_2, $\cdots$, m_s 的和, 而 n 可以分成 t 个正整数 n_1, n_2, $\cdots$, n_t 的和:
$$m=m_1+m_2+\cdots+m_s,\quad n=n_1+n_2+\cdots+n_t.$$
用 $A_{ij}(1\leqslant i\leqslant s,\ 1\leqslant j\leqslant t)$ 表示将 A 中除了第
$$m_1+m_2+\cdots+m_{i-1}+1,\ m_1+m_2+\cdots+m_{i-1}+2,$$
$$\cdots,\ m_1+m_2+\cdots+m_{i-1}+m_i$$
行以外其余的行都划去, 同时将 A 中除了第
$$n_1+n_2+\cdots+n_{j-1}+1,\ n_1+n_2+\cdots+n_{j-1}+2,$$
$$\cdots,\ n_1+n_2+\cdots+n_{j-1}+n_j$$
列以外其余的列都划去, 剩下的 m_in_j 个元素组成的 $m_i\times n_j$ 矩阵, 那么可以将 A 写作
$$A=\begin{pmatrix}A_{11}&A_{12}&\cdots&A_{1t}\\A_{21}&A_{22}&\cdots&A_{2t}\\\cdots&\cdots&\cdots&\cdots\\A_{s1}&A_{s2}&\cdots&A_{st}\end{pmatrix}.$$

更设 B 是 F 上的 $n\times l$ 矩阵，并假定 l 分成了 r 个正整数 l_1, l_2, $\cdots$, l_r 的和：

$$l=l_1+l_2+\cdots+l_r.$$

用 $B_{jk}(1\leqslant j\leqslant s,\ 1\leqslant k\leqslant r)$ 表示将 B 中除了第

$$n_1+n_2+\cdots+n_{j-1}+1,\ n_1+n_2+\cdots+n_{j-1}+2,$$
$$\cdots,\ n_1+n_2+\cdots+n_{j-1}+n_j$$

行以外其余的行都划去，同时将 B 中除了第

$$l_1+l_2+\cdots+l_{k-1}+1,\ l_1+l_2+\cdots+l_{k-1}+2,$$
$$\cdots,\ l_1+l_2+\cdots+l_{k-1}+l_k$$

列以外其余的列都划去，剩下的 n_jl_k 个元素组成的 $n_j\times l_k$ 矩阵．那么可以将 B 写作

$$B=\begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1r} \\ B_{21} & B_{22} & \cdots & B_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ B_{t1} & B_{t2} & \cdots & B_{tr} \end{pmatrix}.$$

于是有分块矩阵的乘法公式

$$AB=(C_{ik})_{1\leqslant i\leqslant s,1\leqslant k\leqslant r},$$

其中
$$C_{ik}=\sum_{j=1}^{t} A_{ij}B_{jk},$$

而上式中乘法和加法分别是矩阵乘法和加法．

分块矩阵同样也有一个加法公式．但比乘法要简单得多，我们就不写出来了．

最后我们引进线性映射的概念，这又给出矩阵的一个几何解释．

定义 1 设 V 和 W 是 F 上的两个向量空间．从 V 映入 W 的一个映射 σ

$$\sigma:\ V\to W$$

叫做从 V 到 W 之中的一个线性映射，如果它满足以下两个

条件：

i) 对任意 $\mathbf{v}_1, \mathbf{v}_2 \in V$，都有

$$\sigma(\mathbf{v}_1+\mathbf{v}_2)=\sigma(\mathbf{v}_1)+\sigma(\mathbf{v}_2).$$

ii) 对任意 $c\in F$ 和 $\mathbf{v}\in V$，都有

$$\sigma(c\mathbf{v})=c\sigma(\mathbf{v}).$$

例如，任意给了 F 上的一个 $m\times n$ 矩阵

$$A=(a_{ij})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n},$$

那么从 $V_m(F)$ 到 $V_n(F)$ 的映射

$$(a_1, a_2, \cdots, a_m)\to(a_1, a_2, \cdots, a_m)A$$

就是一个线性映射；同样从 $V_n(F)$ 到 $V_m(F)$ 的映射

$$(a_1, a_2, \cdots, a_n)\to(a_1, a_2, \cdots a_n)A'$$

也是一个线性映射.

现在设 V 是 F 上的 m 维向量空间，而 W 是 n 维向量空间. 选定 V 的一组基 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_m\}$ 和 W 的一组基 $\{\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_n\}$. 再设 σ 是从 V 到 W 的一个线性映射. 如果 $\sigma(\mathbf{e}_1), \sigma(\mathbf{e}_2), \cdots, \sigma(\mathbf{e}_m)$ 已知，因 V 中任意一个向量 $\mathbf{v}$ 可表成 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_m$ 的线性组合

$$\mathbf{v}=a_1\mathbf{e}_1+a_2\mathbf{e}_2+\cdots+a_m\mathbf{e}_m, \ a_i\in F,$$

而 σ 是线性映射，所以

$$\sigma(\mathbf{v})=a_1\sigma(\mathbf{e}_1)+a_2\sigma(\mathbf{e}_2)+\cdots+a_m\sigma(\mathbf{e}_m). \qquad (14)$$

因此 σ 由 $\sigma(\mathbf{e}_1), \sigma(\mathbf{e}_2), \cdots, \sigma(\mathbf{e}_m)$ 完全确定. 因 $\sigma(\mathbf{e}_i)$ $(1\leqslant i\leqslant m)$ 都是 W 中的向量，可将它们表成 $\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_n$ 的线性组合：

$$\sigma(\mathbf{e}_i)=\sum_{j=1}^{n} a_{ij}\mathbf{f}_j, \ a_{ij}\in F, \ i=1, 2, \cdots, m. \qquad (15)$$

那么 σ 就确定了一个 $m\times n$ 矩阵

$$A=(a_{ij})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}. \qquad (16)$$

A 叫做线性映射 σ 的矩阵. 反过来，σ 由矩阵 A 唯一确定.

实际上，给了一个 $m\times n$ 矩阵 (16)，(14) 和 (15) 式就唯一确定了线性映射 σ. 因此矩阵就成为研究线性映射的重要工具.

从 V 到 W 的线性映射 σ 所确定的矩阵 (16) 显然依赖于 V 的基$\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_m\}$和 W 的基$\{\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_n\}$的选取. 现在在 V 中另选一组基$\{\mathbf{e}'_1, \mathbf{e}'_2, \cdots, \mathbf{e}'_m\}$，并在$W$ 中另选一组基$\{\mathbf{f}'_1, \mathbf{f}'_2, \cdots, \mathbf{f}'_n\}$. 设

$$\sigma(\mathbf{e}'_i)=\sum_{j=1}^{n} b_{ij}\mathbf{f}'_j,\ b_{ij}\in F,\ i=1,\ 2,\ \cdots,\ n. \tag{17}$$

那么 σ 相对于 V 的基$\{\mathbf{e}'_1, \mathbf{e}'_2, \cdots, \mathbf{e}'_m\}$ 和 W 的基$\{\mathbf{f}'_1, \mathbf{f}'_2, \cdots, \mathbf{f}'_n\}$又确定了一个 $m\times n$ 矩阵

$$B=(b_{ij})_{1<i<m,1<j<n}.$$

我们来研究 A 和 B 的关系. 根据定理 1，可设

$$\mathbf{e}'_i=\sum_{k=1}^{m} p_{ik}\mathbf{e}_k,\ i=1,\ 2,\ \cdots,\ m,$$

$$\mathbf{f}_l=\sum_{l=1}^{n} q_{lj}\mathbf{f}'_j,\ l=1,\ 2,\ \cdots,\ n,$$

其中 $$P=(p_{ik})_{1<i,k<m},\ Q=(q_{lj})_{1<l,j<n}.$$

分别是 F 上的 $m\times m$ 可逆矩阵和 $n\times n$ 可逆矩阵. 我们有

$$\begin{aligned}\sigma(\mathbf{e}'_i)&=\sum_{k=1}^{m} p_{ik}\sigma(\mathbf{e}_k)=\sum_{k=1}^{m} p_{ik}\sum_{l=1}^{n} a_{kl}\mathbf{f}_l\\&=\sum_{k=1}^{m} p_{ik}\sum_{l=1}^{n} a_{kl}\sum_{j=1}^{n} q_{lj}\mathbf{f}'_j\\&=\sum_{j=1}^{n}\left(\sum_{k=1}^{m}\sum_{l=1}^{n} p_{ik}a_{kl}q_{lj}\right)\mathbf{f}'_j\end{aligned} \tag{18}$$

比较(17)，(18)两式，得

$$b_{ij}=\sum_{k=1}^{m}\sum_{l=1}^{n} p_{ik}a_{kl}q_{lj},\quad i=1,\ 2,\ \cdots,m;\ j=1,2\cdots,n \tag{19}$$

再根据矩阵乘法的定义，(19)式即表明

$$B=PAQ \tag{20}$$

定义 2 设 A 和 B 是 F 上的两个 $m\times n$ 矩阵．如果有 F 上的 $m\times m$ 可逆矩阵 P 和 $n\times n$ 可逆矩阵 Q 存在，使得(20)式成立，我们就说 A 与 B 等价．

根据上面的讨论可知，从 V 映入 W 的一个线性映射相对于 V 和 W 中不同的基所确定的矩阵一定等价．

定理 4 设 A 是 F 上的 $m\times n$ 矩阵，并假定 A 的秩等于 r．那么 A 一定和下面这个矩阵等价：

$$\begin{pmatrix} I^{(r)} & 0 \\ 0 & 0^{(m-r,\,n-r)} \end{pmatrix} \tag{21}$$

证．根据§2 定理 5 和本节定理 3 的系理 2，有 $m\times m$ 可逆矩阵 P 存在，使 PA 是阶梯形矩阵

$$A_0=\left(\begin{array}{ccccccccc}
0\cdots0 & 1 & *\cdots* & 0 & *\cdots* & 0 & *\cdots* & \cdots\ 0 & *\cdots* \\
0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & 0 & *\cdots* & \cdots\ 0 & *\cdots* \\
0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & \cdots\ 0 & *\cdots* \\
\cdots & & \cdots & & \cdots & & \cdots & & \cdots \\
0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & \cdots\ 1 & *\cdots* \\
0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & \cdots\ 0 & 0\cdots0 \\
\cdots & & \cdots & & \cdots & & \cdots & & \cdots \\
0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & \cdots\ 0 & 0\cdots0
\end{array}\right)
\begin{array}{l}
\left.\begin{matrix}\\ \\ \\ \\ \\ \end{matrix}\right\} r\text{ 行} \\
\left.\begin{matrix}\\ \\ \\ \end{matrix}\right\} n-r\text{ 行}
\end{array}$$

可设 A_0 的第 i 行 $(1\leqslant i\leqslant r)$ 的第一个不等于 0 的元素 1 位于第 k_i 列，而 $1\leqslant k_1<k_2<\cdots<k_r\leqslant n$．把 A_0 的 (i,k) 位置的元素记作 a_{ik}．那么将 A_0 从后面乘以 $n\times n$ 的第二种初等矩阵 P_{1k_1} 之后，再从后面乘以 $n\times n$ 的第三种初等矩阵之积．

$$\prod_{i_1=k_1+1}^{k_2-1} T_{i_1 1}(-a_{1i_1})\cdot\prod_{i_2=k_2+1}^{k_3-1} T_{i_2 1}(-a_{1i_2})\cdot\cdots\cdot\prod_{i_r=k_r+1}^{n} T_{1i_r}(-a_{1i_r})$$

(注意，当某个 $a_{1i_s}=0$ 时，$T_{i_s1}(a_{1i_s})=I$)，就将 A_0 的第一行变成

$$(1\ \underbrace{0\ 0\cdots 0}_{n-1\text{个}0})$$

而 A_0 的其余各行保持不动，把这样得到的矩阵记作 A_1. 再将 A_1 后面乘以 $n\times n$ 的第二种初等矩阵 P_{2k_2} 之后，从后面再乘以 $n\times n$ 的第三种初等矩阵之积

$$\prod_{i_2=k_2+1}^{k_3-1} T_{i_22}(-a_{2i_2})\cdots\cdots\prod_{i_r=k_r+1}^{n} T_{2i_r}(-a_{2i_r}),$$

就将 A_1 的第二行变成

$$(0\ 1\ \underbrace{0\ 0\cdots 0}_{n-2\text{个}0}).$$

而 A_1 的其余各行(包括第一行)保持不动，如此继续下去，可见将 A_0 从后面乘以若干个 $n\times n$ 初等矩阵的乘积之后，可将 A_0 化成(21). 因初等矩阵的乘积是可逆矩阵，故有 $n\times n$ 可逆矩阵 Q 存在使 $PAQ=A_0Q$ 即为矩阵(21).

系理 F 上的两个 $m\times n$ 矩阵 A 和 B 等价，当且仅当它们有相同的秩.

矩阵(21)叫做秩为 r 的 $m\times n$ 矩阵在等价变换下的标准形.

现在设 σ 是 F 上的 n 维向量空间 V 到它自身之中的一个线性映射. 选定 V 的一组基 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$. 因 $\sigma(\mathbf{e}_1)$, $\sigma(\mathbf{e}_2)$, $\cdots$, $\sigma(\mathbf{e}_n)$都是 V 中向量，可将它们表成 $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ 的线性组合:

$$\sigma(\mathbf{e}_i)=\sum_{j=1}^{n} a_{ij}\mathbf{e}_j,\ a_{ij}\in F,\ i=1,\ 2,\ \cdots,\ n. \tag{22}$$

这样，相对于基 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$，$\sigma$ 就确定了一个 $n\times n$ 矩阵

$$A=(a_{ij})_{1\leqslant i,j\leqslant n}.$$

A 叫做线性映射 σ 相对于基 $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ 的矩阵. 反过来,

σ 也由矩阵 A 唯一确定. 再设$\{\mathbf{e}_1', \mathbf{e}_2', \cdots, \mathbf{e}_n'\}$也是$V$的一组基,并设

$$\sigma(\mathbf{e}_i')=\sum_{j=1}^{n} b_{ij}\mathbf{e}_j',\ b_{ij}\in F,\ i=1,\ 2,\ \cdots,\ n. \tag{23}$$

那么相对于基$\{\mathbf{e}_1', \mathbf{e}_2', \cdots, \mathbf{e}_n'\}$, σ 又确定了一个 $n\times n$ 矩阵

$$B=(b_{ij})_{1\leq i,j\leq n}.$$

我们来研究 A 和 B 的关系. 根据定理 1 及其证明, 可设

$$\mathbf{e}_i=\sum_{j=1}^{n} p_{ij}\mathbf{e}_j',\quad \mathbf{e}_i'=\sum_{j=1}^{n} q_{ij}\mathbf{e}_j,\quad i=1,\ 2,\ \cdots,\ n,$$

而
$$P=(p_{ij})_{1\leq i,j\leq n},\quad Q=(q_{ij})_{1\leq i,j\leq n}$$

是互为逆矩阵的 $n\times n$ 可逆矩阵, 即

$$PQ=QP=I^{(n)}.$$

我们有

$$\begin{aligned}\sigma(\mathbf{e}_i')&=\sum_{j=1}^{n} q_{ij}\sigma(\mathbf{e}_j)=\sum_{j=1}^{n} q_{ij}\sum_{k=1}^{n} a_{jk}\mathbf{e}_k\\&=\sum_{j=1}^{n} q_{ij}\sum_{k=1}^{n} a_{jk}\sum_{l=1}^{n} p_{kl}\mathbf{e}_l'\\&=\sum_{l=1}^{n}\left(\sum_{j=1}^{n}\sum_{k=1}^{n} q_{ij}a_{jk}p_{kl}\right)\mathbf{e}_l'\end{aligned} \tag{24}$$

比较(23), (24)两式, 得到

$$b_{il}=\sum_{j=1}^{n}\sum_{k=1}^{n} q_{ij}a_{jk}p_{kl},\ i,\ l=1,\ 2,\ \cdots,\ n.$$

即
$$B=QAP=P^{-1}AP.$$

定义 3 F 上两个 $n\times n$ 矩阵 A 和 B 叫做相似, 如果有 F 上 $n\times n$ 可逆矩阵 P 存在, 使得 $B=P^{-1}AP$.

根据上面的讨论可知, 从 V 映入它自身之中的一个线性映射相对于 V 的不同的基所确定的矩阵一定相似. 关于矩阵在相似下的标准形, 将在本章最末一节中讨论.

§4 线性方程组

设 F 是任意一个域，$a_{ij}(i=1, 2, \cdots, m;\ j=1, 2, \cdots, n)$ 和 $b_i(i=1, 2, \cdots, m)$ 都是 F 中的元素，而 $x_1, x_2, \cdots, x_n$ 是 n 个文字，那么

$$\left.\begin{array}{l} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=b_1 \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n=b_m \end{array}\right\} \tag{1}$$

就叫做 n 个文字 $x_1, x_2, \cdots, x_n$ 的 m 个方程的线性方程组. 采用矩阵记号，令

$$A=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n},$$
$$\mathbf{x}=(x_1, x_2, \cdots, x_n),$$
$$\mathbf{b}=(b_1, b_2, \cdots, b_m).$$

那么方程组(1)可以写成下面的简式

$$A\mathbf{x}'=\mathbf{b}'. \tag{2}$$

注意，这里 $\mathbf{x}'$ 表示将 $\mathbf{x}$ 看作 $1\times n$ 矩阵的转置矩阵，而 $\mathbf{b}'$ 表示将 $\mathbf{b}$ 看作 $1\times m$ 矩阵的转置矩阵. 所谓求线性方程组(2)的解，就是在 F 中求出 n 个元素 $c_1, c_2, \cdots, c_n$，将它们代入(1)中 m 个方程里，结果得到 m 个等式；换句话说，令

$$\mathbf{c}=(c_1, c_2, \cdots, c_n),$$

如果
$$A\mathbf{c}'=\mathbf{b}',$$

我们就说 $c_1, c_2, \cdots, c_n$ 是(1)(或(2))的一组解，也说 $\mathbf{c}$ 是(1)(或(2))的一个解向量.

当 $b_1=b_2=\cdots=b_m=0$ 时，(1)和(2)又叫齐次线性方程组；否则就叫非齐次线性方程组.

我们先讨论齐次线性方程组. 用 $\mathbf{0}$ 表示分量都等于0的

m维行向量

$$\mathbf{0}=(\underbrace{0,\ 0,\ \cdots,\ 0}_{m\text{个}0}),$$

那么n个文字的m个方程的齐次线性方程组可以写成

$$A\mathbf{x}'=\mathbf{0}',$$

其中A是F上的$m\times n$矩阵.

定理1 设F是一个域，$A=(a_{ij})_{1\leq i\leq m,1\leq j\leq n}$是$F$上的一个$m\times n$矩阵，那么齐次线性方程组

$$A\mathbf{x}'=\mathbf{0}' \tag{3}$$

的解向量的全体组成$V_n(F)$的一个子空间. 如果rank $A=r$，这个子空间就是$n-r$维的.（这个子空间叫做线性方程组(3)的解空间.）

证. 设

$$\mathbf{c}=(c_1,\ c_2,\ \cdots,\ c_n),\ \mathbf{d}=(d_1,\ d_2,\ \cdots,\ d_n)$$

是(3)的两个解向量，即

$$A\mathbf{c}'=\mathbf{0}',\quad A\mathbf{d}'=\mathbf{0}',$$

那么

$$A(\mathbf{c}+\mathbf{d})'=A(\mathbf{c}'+\mathbf{d}')=A\mathbf{c}'+A\mathbf{d}'=\mathbf{0}'+\mathbf{0}'=\mathbf{0}'.$$

因此$\mathbf{c}+\mathbf{d}$也是(3)的解向量. 又如果$\mathbf{c}$是(3)的解向量，即$A\mathbf{c}'=0$，而$a\in F$，那么

$$A(a\mathbf{c})'=A(a\mathbf{c}')=a(A\mathbf{c}')=a\cdot\mathbf{0}'=\mathbf{0}'.$$

因此$a\mathbf{c}$也是(3)的解向量. 于是根据§1定理4知，(3)的解向量的全体组成$V_n(F)$的一个子空间.

我们再证明，如果P是F上的$m\times m$可逆矩阵，那么齐次线性方程组(3)的解空间与

$$(PA)\mathbf{x}'=\mathbf{0}'$$

的解空间一致. 实际上，设$A\mathbf{c}'=\mathbf{0}'$，那么显然有

$$(PA)\mathbf{c}'=P(A\mathbf{c}')=P\mathbf{0}'=\mathbf{0}'.$$

反过来,设$(PA)\mathbf{c}'=\mathbf{0}$,并设$P^{-1}$是$P$的逆矩阵,那么

$$
\begin{aligned}
A\mathbf{c}' &= (IA)\mathbf{c}' = ((P^{-1}P)A)\mathbf{c}' = (P^{-1}(PA))\mathbf{c}' \\
&= P^{-1}((PA)\mathbf{c}') = P^{-1}\mathbf{0}' = \mathbf{0}'.
\end{aligned}
$$

设$\operatorname{rank} A=r$,那么根据§3定理5可知,有$m\times m$可逆矩阵P存在,使$PA=A_0$是阶梯形矩阵:

$$
A_0=\begin{pmatrix}
0\cdots0 & 1*\cdots* & 0*\cdots* & 0*\cdots* & \cdots & 0*\cdots* \\
0\cdots0 & 00\cdots0 & 1*\cdots* & 0*\cdots* & \cdots & 0*\cdots* \\
0\cdots0 & 00\cdots0 & 00\cdots0 & 1*\cdots* & \cdots & 0*\cdots* \\
\cdots & \cdots & \cdots & \cdots & & \cdots \\
0\cdots0 & 00\cdots0 & 00\cdots0 & 00\cdots0 & \cdots & 1*\cdots* \\
0\cdots0 & 00\cdots0 & 00\cdots0 & 00\cdots0 & \cdots & 00\cdots0 \\
 & \cdots & \cdots & \cdots & & \cdots \\
0\cdots0 & 00\cdots0 & 00\cdots0 & 00\cdots0 & \cdots & 00\cdots0
\end{pmatrix}
\begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \end{matrix}\right\} r\text{行} \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} n-r\text{行} \end{matrix}
\tag{4}
$$

那么(3)的解空间与

$$A_0\mathbf{x}'=\mathbf{0}' \tag{5}$$

的解空间一致,因此要证明(3)的解空间是$n-r$维的,只要证明(5)的解空间是$n-r$维的就行了.

设A_0的第i行$(1\leqslant i\leqslant r)$中从左往右数第一个等于1的元素在第$k_i$列,那么

$$1\leqslant k_1<k_2<\cdots<k_r\leqslant n.$$

注意,从A_0的形状可以看出,当任意选定$V_n(F)$中一个向量$\mathbf{c}$的第1, 2, …, k_1-1, k_1+1, k_1+2, …, k_2-1, k_2+1, k_2+2, …, k_3-1, …, k_r-1, k_r+1, k_r+2, …, n分量c_1, c_2, …, c_{k_1-1}, c_{k_1+1}, c_{k_1+2}, …, c_{k_2-1}, c_{k_2+1}, c_{k_2+2}, …, c_{k_3-1}, …, c_{k_r-1}, c_{k_r+1}, c_{k_r+2}, …, c_n后,从条件$A_0\mathbf{c}'=\mathbf{0}'$可唯一地算出$\mathbf{c}$的第$k_1$, k_2, …, k_r分量c_{k_1}, c_{k_2}, …, c_{k_r}. 实际上,设(5)的第i个方程$(1\leqslant i\leqslant r)$是

$$
\begin{aligned}
& x_{k_i}+a^{(0)}_{ik_i+1}x_{k_i+1}+\cdots+a^{(0)}_{ik_{i+1}-1}x_{k_{i+1}-1}+a^{(0)}_{ik_{i+1}+1}x_{k_{i+1}+1} \\
&\quad +\cdots+a^{(0)}_{ik_{i+2}-1}x_{k_{i+2}-1}+\cdots+a^{(0)}_{ik_r+1}x_{k_r+1}+\cdots+a^{(0)}_{in}x_n=0,
\end{aligned}
$$

那么

$$c_{k_i}=-(a_{ik_{i+1}}^{(0)}c_{k_{i+1}}+\cdots+a_{ik_{i+1}-1}^{(0)}c_{k_{i+1}-1}+a_{ik_{i+1}+1}^{(0)}c_{k_{i+1}+1}$$
$$+\cdots+a_{ik_{i+2}-1}^{(0)}c_{k_{i+2}-1}+\cdots+a_{ik_r+1}^{(0)}c_{k_r+1}+\cdots+a_{in}^{0}c_n).$$

由此立刻推出(5)的解空间的维数是 $n-r$.

值得注意的是，定理1的证明实际上给出了求齐次方程组(3)的解空间的一个方法，这个方法的核心是§2定理5中介绍的消去法.

定理2 设 W 是 $V_n(F)$ 的一个子空间. 令

$$W^*=\{\mathbf{v}\mid\mathbf{v}\in V_n(F)\text{ 而 }\mathbf{v}\cdot\mathbf{w}'=0\text{ 对一切 }\mathbf{w}\in W\},$$

那么 W^* 也是 $V_n(F)$ 的一个子空间. 更进一步，如果 $\dim W=r$，那么 $\dim W^*=n-r$. 由此推出 $(W^*)^*=W$.（我们把 W^* 叫做 W 的对偶子空间.）

证. W^* 是 $V_n(F)$ 的子空间这一点的证明完全同定理1中(3)的解向量的全体是一子空间的证明一样，因而略去.

设 $\dim W=r$，并设 $\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_r$ 是 W 的一组基. 令

$$A=\begin{pmatrix}\mathbf{w}_1\\ \mathbf{w}_2\\ \vdots\\ \mathbf{w}_r\end{pmatrix},$$

那么 A 是个 $r\times n$ 矩阵而 $\operatorname{rank}A=r$. 如果 $\mathbf{v}\in W^*$，那么显然有

$$\mathbf{v}\mathbf{w}_i'=0,\ i=1, 2, \cdots, r. \tag{6}$$

将上式求转置就得到

$$\mathbf{w}_i\mathbf{v}'=0,\ i=1, 2, \cdots, r, \tag{7}$$

于是

$$A\mathbf{v}'=\mathbf{0}'. \tag{8}$$

这就是说 $\mathbf{v}$ 属于齐次线性方程组

$$A\mathbf{x}'=\mathbf{0}' \tag{9}$$

的解空间. 反过来,如果 $\mathbf{v}$ 属于(9)的解空间, 即(8)式成立, 那么(7)式成立, 因而(6)式成立. 因$\{\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_r\}$是 W 的一组基, 所以 W 中任一向量 $\mathbf{w}$ 都可以表成它们的线性组合

$$\mathbf{w}=c_1\mathbf{w}_1+c_2\mathbf{w}_2+\cdots+c_r\mathbf{w}_r,\ c_i\in F,$$

那么根据(5)就有

$$\begin{aligned}\mathbf{v}\mathbf{w}'&=\mathbf{v}(c_1\mathbf{w}_1+c_2\mathbf{w}_2+\cdots+c_r\mathbf{w}_r)'\\&=\mathbf{v}(c_1\mathbf{w}_1')+\mathbf{v}(c_2\mathbf{w}_2')+\cdots+\mathbf{v}(c_r\mathbf{w}_r')\\&=c_1(\mathbf{v}\mathbf{w}_1')+c_2(\mathbf{v}\mathbf{w}_2')+\cdots+c_r(\mathbf{v}\mathbf{w}_r')\\&=c_1\mathbf{0}'+c_2\mathbf{0}'+\cdots+c_r\mathbf{0}'=\mathbf{0}',\end{aligned}$$

因此 $\mathbf{v}\in W^*$. 这证明了 W^* 与 (9) 的解空间一致, 根据定理 1, (9)的解空间是 $n-r$ 维的, 所以 $\dim W^*=n-r$.

显然有 $W\subset(W^*)^*$. 设 $\dim W=r$, 那么 $\dim W^*=n-r$, 于是 $\dim(W^*)^*=n-(n-r)=r$. 因此根据 §1 定理 5 就一定有 $(W^*)^*=W$.

这样定理 2 就完全证明了.

下面来讨论非齐次线性方程组. 我们先证明

定理 3 设 F 是一个域, $A=(a_{ij})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ 是 F 上的一个 $m\times n$ 矩阵, $\mathbf{b}=(b_1, b_2, \cdots, b_m)$是 $V_m(F)$ 中的一个向量. 用 W 表示齐次线性方程组

$$A\mathbf{x}'=\mathbf{0}' \tag{3}$$

的解空间. 如果 $\mathbf{d}=(d_1, d_2, \cdots, d_n)$是非齐次线性方程组

$$A\mathbf{x}'=\mathbf{b}' \tag{2}$$

的一组解, 那么

$$\mathbf{d}+W=\{\mathbf{d}+\mathbf{c}\mid \mathbf{c}\in W\}$$

就是(2)的全部解的集合.

证. 设 $\mathbf{c}\in W$, 即 $A\mathbf{c}'=\mathbf{0}'$. 那么

$$A(\mathbf{d}+\mathbf{c})'=A(\mathbf{d}'+\mathbf{c}')=A\mathbf{d}'+A\mathbf{c}'$$
$$=\mathbf{b}'+\mathbf{0}'=\mathbf{b}'.$$

这证明了 $\mathbf{d}+W$ 中的向量都是(2)的解向量.

反过来, 设 $\mathbf{d}_1$ 是(2)的一个解向量, 即 $A\mathbf{d}_1'=0$, 那么

$$A(\mathbf{d}_1-\mathbf{d})'=A(\mathbf{d}_1'-\mathbf{d}')=A\mathbf{d}_1'-A\mathbf{d}'$$
$$=\mathbf{b}'-\mathbf{b}'=\mathbf{0}'.$$

这就是说 $\mathbf{d}_1-\mathbf{d}\in W$. 设 $\mathbf{d}_1-\mathbf{d}=\mathbf{c}\in W$, 那么

$$\mathbf{d}_1=\mathbf{d}+\mathbf{c}\in\mathbf{d}+W.$$

我们附带提一下, 如果采用陪集的语言, 定理 3 可以说成: 如果非齐次方程组(2)有解, 那么它的解的全体就是齐次方程组(2)的解空间的一个陪集.

问题是非齐次方程组(2)是否一定有解. 我们有下面的定理.

定理 4 设 F 是一个域, $A=(a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ 是 F 上的一个 $m\times n$ 矩阵, $\mathbf{b}=(b_1, b_2, \cdots, b_m)\in V_m(F)$. 令

$$B=(A, \mathbf{b}'),$$

那么非齐次线性方程组

$$A\mathbf{x}'=\mathbf{b}' \tag{2}$$

有解, 当且仅当 $\operatorname{rank} A=\operatorname{rank} B$.

证. 设 P 是个 $m\times m$ 可逆矩阵, 那么仿照定理 1 的证明可证(2)有解, 当且仅当

$$(PA)\mathbf{x}'=P\mathbf{b}'$$

有解. 根据 §2 定理 2, 有可逆矩阵 P 存在, 使 $PB=B_0$ 是阶梯形矩阵. 写

$$B_0=(A_0, \mathbf{b}_0')$$

其中 $A_0=PA$, $\mathbf{b}_0'=P\mathbf{b}'$. 显然 $\operatorname{rank} A=\operatorname{rank} A_0$, $\operatorname{rank} B=\operatorname{rank} B_0$. 看(2)是否有解, 只要看

$$A_0\mathbf{x}'=\mathbf{b}_0' \tag{10}$$

是否有解.

设 $\operatorname{rank} A=r$, 并设 A_0 的形状是(4). 至于 $\mathbf{b}_0'$, 有两种情形可能发生:

1)
$$\mathbf{b}_0'=\begin{pmatrix} * \\ * \\ \vdots \\ * \\ 0 \\ \vdots \\ 0 \end{pmatrix}\begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} r\text{ 个} \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} n-r\text{ 个} \end{matrix}$$

这时 $\operatorname{rank} B_0=\operatorname{rank} A_0$. 和定理 1 的证明中完全一样, 任意选定 $V_n(F)$ 中一个向量 $\mathbf{c}$ 的第 1, 2, …, k_1-1, k_1+1, $k_1+2, \cdots, k_2-1$, k_2+1, k_2+2, …, k_3-1, …, k_r-1, k_r+1, k_r+2, …, n 分量 $c_1, c_2, \cdots, c_{k_1-1}, c_{k_1+1}, c_{k_1+2}, \cdots, c_{k_2-1}, c_{k_2+1}, c_{k_2+2}, \cdots, c_{k_3-1}, \cdots, c_{k_r-1}, c_{k_r+1}, c_{k_r+2}, \cdots, c_n$ 后, 从条件 $A_0\mathbf{c}'=\mathbf{b}_0'$ 可唯一地定出 $\mathbf{c}$ 的第 $k_1, k_2, \cdots, k_r$ 分量 $c_{k_1}, c_{k_2}, \cdots, c_{k_r}$. 因此这时(10)有解.

2)
$$\mathbf{b}_0'=\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\text{第 } r+1 \text{ 个分量.}$$

这时 $\operatorname{rank} B_0=r+1>\operatorname{rank} A_0$. 于是 $\operatorname{rank} B>\operatorname{rank} A$. 而(10)的第 $r+1$ 个方程是

$$0x_1+0x_2+\cdots+0x_n=1.$$

显然 $V_n(F)$ 中任一向量均不满足上述方程. 因此这时 (10) 无解.

这样定理 4 就完全证明了.

值得指出的是，定理 4 的证明实际上给出了求非齐次方程组(2)的解向量的一个方法，这个方法的核心是用 §2 定理 5 中介绍的将 $B=(A, \mathbf{b}')$ 化成阶梯形矩阵的消去法.

定理 5 设 F 是域，A 是 F 上的 $n\times n$ 矩阵，而 $\mathbf{b}\in V_n(F)$，那么非齐次线性方程组

$$A\mathbf{x}'=\mathbf{b}' \tag{11}$$

有唯一一组解，当且仅当 $\operatorname{rank} A=n$.

证. 设(11)有唯一一组解. 根据定理 3 可知，这时 $A\mathbf{x}'=\mathbf{0}'$ 的解空间仅由 $V_n(F)$ 中的零向量 $\mathbf{0}=(0, 0, \cdots, 0)$ 组成，即 $A\mathbf{x}'=\mathbf{0}'$ 的解空间是 0 维的. 再根据定理1，就有 $\operatorname{rank} A=n$.

反之，设 $\operatorname{rank} A=n$. 因 $B=(A, \mathbf{b}')$ 只有 n 行，所以

$$n\geqslant \operatorname{rank}(A, \mathbf{b}')$$

但显然如果 A 的 $i_1, i_2, \cdots, i_r$ 行线性无关，那么 $B=(A, \mathbf{b}')$ 的 $i_1, i_2, \cdots, i_r$ 行也线性无关. 所以

$$\operatorname{rank}(A, \mathbf{b}')\geqslant \operatorname{rank} A=n.$$

因此
$$\operatorname{rank} B=\operatorname{rank} A=n.$$

那么根据定理 4 可知，(11)一定有解. 仍因 $\operatorname{rank} A=n$，所以根据定理 1 知 $A\mathbf{x}'=\mathbf{0}'$ 的解空间是 0 维的. 于是根据定理 3 知(11)只有唯一的一组解.

§5 行 列 式

行列式是许多读者都熟悉的内容. 为了便于查找，我们把它的定义和重要性质列举出来，而不加证明. 然后再介绍以后要用到的几个定理.

定义 1 设 $i_1, i_2, \cdots, i_n$ 是 $1, 2, \cdots, n$ 这 n 个数的一个排列，即 $1\leqslant i_1, i_2, \cdots, i_n\leqslant n$，而 $i_1, i_2, \cdots, i_n$ 两两不同. 如果在排列 $i_1, i_2, \cdots, i_n$ 中有一对数 i_j 和 i_k $(j\neq k)$ 有性质 $i_j>i_k$

而 $j<k$, 那么就把这对数叫做一个逆序. 一个排列中逆序的总数就叫做这个排列的逆序数. 用 $\varepsilon(i_1, i_2, \cdots, i_n)$ 来代表排列 $i_1, i_2, \cdots, i_n$ 的逆序数.

定义 2 设 F 是一个域, 而

$$A=(a_{ij})_{1\leqslant i,j\leqslant n} \tag{1}$$

是 F 上的一个 $n\times n$ 矩阵, 那么 A 的行列式

$$|A|=\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

就定义为下面的和式

$$\sum_{j_1, j_2, \cdots, j_n} (-1)^{\varepsilon(j_1, j_2, \cdots, j_n)} a_{1j_1} a_{2j_2} \cdots a_{nj_n},$$

其中求和号是对 1, 2, …, n 这 n 个数的所有的 $n!$ 个排列求和. 因此上面和式中一共有 $n!$ 项.

显然 A 的行列式是 F 中的元素.

定义 3 设 A 是域 F 上的一个 $n\times n$ 矩阵. 如果 $|A|=0$, A 就叫奇异矩阵. 如果 $|A|\neq 0$, A 就叫非异矩阵.

行列式有下面一系列的性质, 这些性质对于计算行列式非常有用. 以下总设 A 是 F 上的 $n\times n$ 矩阵(1).

性质 1 $|A|=|A'|$, 即

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{vmatrix}.$$

性质 2 将 A 的某一行乘以 F 中任一元素 c, 所得矩阵的行列式等于 $c|A|$, 即

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ ca_{i1} & ca_{i2} & \cdots & ca_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = c \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}.$$

性质 3 将 A 的某两行对调，所得矩阵的行列式等于 $-|A|$，即

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = - \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}.$$

特别，当 F 的特征为 2 时，将 A 的某两行对调，行列式不变.

性质 4 将 A 的某一行加上另一行乘以 F 中的任一元素 d，行列式不变，即

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{j1}+da_{i1} & a_{j2}+da_{i2} & \cdots & a_{jn}+da_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}.$$

性质 2, 3, 4 实际上说的是作用在一个 $n\times n$ 矩阵 A 的行上的初等变换对 A 的行列式的影响. 计算矩阵 A 的行列式的一个方法就是用行的初等变换把 A 化成阶梯形矩阵，而 $n\times n$ 阶梯形矩阵的行列式等于 0 或 1，要看它的主对角线上有没有 0 而定. 有时对矩阵 A 的行进行初等变换，不必等到

将 A 化成阶梯形矩阵，而利用下面的性质 5 就可以判断 A 的行列式等于 0. 性质 5 实际上是性质 2 和 4 的推论.

性质 5 如果 A 的某一行等于另一行乘以 F 中的任一元素 c，那么 $|A|=0$，即

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ ca_{i1} & ca_{i2} & \cdots & ca_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}=0.$$

特别，如果 A 有两行一样，或 A 有一行的元素全都是 0，那么 $|A|=0$.

定义 4 设 A 是 F 上的 $n\times n$ 矩阵，写

$$A=(a_{ij})_{1\leq i,j\leq n}.$$

将 A 的第 i 行和第 j 列的元素划去以后，得到一个 $(n-1)\times(n-1)$ 矩阵，这个矩阵的行列式记作 M_{ij}. 令

$$A_{ij}=(-1)^{i+j}M_{ij},$$

那么 A_{ij} 叫做 A 中 (i, j) 位置元素 a_{ij} 的代数余子式，即

$$A_{ij}=(-1)^{i+j}\begin{vmatrix} a_{11} & \cdots & a_{1j-1} & a_{1j+1} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{i-11} & \cdots & a_{i-1j-1} & a_{i-1j+1} & \cdots & a_{i-1n} \\ a_{i+11} & \cdots & a_{i+1j-1} & a_{i+1j+1} & \cdots & a_{i+1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nj-1} & a_{nj+1} & \cdots & a_{nn} \end{vmatrix}.$$

性质 6 对 $i=1, 2, \cdots, n$，都有

$$a_{i1}A_{i1}+a_{i2}A_{i2}+\cdots+a_{in}A_{in}=|A|, \tag{2}$$

而当 $i\neq k$ 时，有

$$a_{i1}A_{k1}+a_{i2}A_{k2}+\cdots+a_{in}A_{kn}=0.$$

(2)式通常说成是，将 A 的行列式按它的第 i 行展开.

上述行列式的性质 2—6 是对矩阵 A 的行来说的. 但因为行列式有性质 1，即将 A 的行列对调，行列式不变，所以对于 A 的列来说同样有性质 2—6. 我们把它们叫做性质2′—6′. 下面我们只举出性质 6′ 来，其他就不一一列举了.

性质 6′ 对 $j=1, 2, \cdots, n$，都有

$$a_{1j}A_{1j}+a_{2j}A_{2j}+\cdots+a_{nj}A_{nj}=|A|, \tag{3}$$

而当 $j\neq k$ 时，有

$$a_{1j}A_{1k}+a_{2j}A_{2k}+\cdots+a_{nj}A_{nk}=0.$$

(3)式通常说成是，将 A 的行列式按它的第 j 列展开.

我们还有

性质 7 设 A, B 都是域 F 上的 $n\times n$ 矩阵，那么

$$|AB|=|A|\cdot|B|.$$

这个性质通常称为行列式的乘法定理.

定义 5 设 A 是域 F 上的 $n\times n$ 矩阵. 矩阵

$$\begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}$$

叫做 A 的伴随矩阵，记作 $\operatorname{adj}A$.

我们有

定理 1 设 A 是域 F 上的 $n\times n$ 矩阵，那么

$$A\cdot\operatorname{adj}A=\operatorname{adj}A\cdot A=|A|I^{(n)}.$$

证. 这实际上是性质 6(对于行)以及 6′(对于列) 的另一说法而已.

从这个定理立刻推出

定理 2 设 A 是域 F 上的 $n\times n$ 矩阵. A 是非异矩阵，当且仅当 A 是可逆矩阵.

证. 设 A 是非异矩阵, 即 $|A|\neq 0$. 令

$$B=|A|^{-1}\operatorname{adj}A,$$

那么根据定理 1 就有

$$AB=BA=I^{(n)}.$$

这就是说 A 是可逆矩阵, 而 B 是 A 的逆.

反过来, 设 A 是可逆矩阵, 即有 $n\times n$ 矩阵 B 使

$$AB=BA=I^{(n)}$$

显然 $|I^{(n)}|=1$. 那么根据性质 7 就有

$$|A|\,|B|=|AB|=|I^{(n)}|=1.$$

所以 $|A|\neq 0$, 即 A 是非异矩阵.

定理 3(克拉姆 (Cramer) 法则) 设 A 是域 F 上的 $n\times n$ 非异矩阵, 而 $\mathbf{b}=(b_1, b_2, \cdots, b_n)\in V_n(F)$, A_j 表示将 A 的第 j 列用 $\mathbf{b}'$ 来代替而得到的矩阵, 那么线性方程组

$$A\mathbf{x}=\mathbf{b}' \tag{4}$$

的唯一的一组解可表作

$$x_j=\frac{|A_j|}{|A|},\quad j=1, 2, \cdots, n. \tag{5}$$

证. 根据 §3 定理 5, 我们知道, 当 A 是非异矩阵时, (4) 有唯一解, 因此只要能证明(5)确是(4)的一组解就行了. 将 $|A_j|$ 按它的第 j 列展开就有

$$|A_j|=b_1A_{1j}+b_2A_{2j}+\cdots+b_nA_{nj}=\sum_{k=1}^{n}b_kA_{kj}.$$

再利用性质 6, 就有

$$\sum_{j=1}^{n}a_{ij}\frac{|A_j|}{|A|}=\frac{1}{|A|}\sum_{j=1}^{n}a_{ij}\sum_{k=1}^{n}b_kA_{kj}$$

$$=\frac{1}{|A|}\sum_{k=1}^{n}b_k\left(\sum_{j=1}^{n}a_{ij}A_{kj}\right)=b_i,\quad i=1, 2, \cdots, n.$$

这就是 $$A\left(\frac{|A_1|}{|A|}, \frac{|A_2|}{|A|}, \cdots, \frac{|A_n|}{|A|}\right)'=\mathbf{b}'.$$

这证明了(5)确实是(4)的一组解.

应该着重指出的是，克拉姆(Cramer)法则只是给出了非齐次线性方程组(4)的解的一种表达方法. 用它来计算(4)的解，当 n 适当大时，计算量很大，因此很不方便. 要计算(4)的解还是用 §3 中介绍的消去法最方便.

定义 6 设 A 是域 F 上的 $n\times n$ 矩阵，x 是一个文字，那么行列式

$$|xI-A|$$

是 $F[x]$ 中的一个 n 次多项式. 这个多项式叫做 A 的**特征多项式**.

定义 7 设 A 是域 F 上的 $n\times n$ 矩阵. 我们说 A **适合** $F[x]$ 中的多项式

$$c_0+c_1x+c_2x^2+\cdots+c_mx^m=0,\ c_i\in F,$$

如果
$$c_0I+c_1A+c_2A^2+\cdots+c_mA^m=0.$$

A 所适合的 $F[x]$ 中非零的次数最低的首项系数为 1 的多项式叫做 A 的**极小多项式**.

定理 4 (凯莱-哈密顿(Cayley-Hamilton)定理)域 F 上的每个 $n\times n$ 矩阵 A 都适合它的特征多项式，即如果将 $|xI-A|$ 表成

$$|xI-A|=x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0,\ a_i\in F,$$

那么

$$A^n+a_{n-1}A^{n-1}+a_{n-2}A^{n-2}+\cdots+a_1A+a_0I=0. \tag{6}$$

证. 根据定理 1，我们有

$$\begin{aligned}(xI-A)\operatorname{adj}(xI-A)&=\operatorname{adj}(xI-A)(xI-A)\\&=|xI-A|I.\end{aligned} \tag{7}$$

$\operatorname{adj}(xI-A)$ 的每个元素 $b_{ij}(1\leqslant i,\ j\leqslant n)$ 都是 x 的次数 $\leqslant n-1$ 的多项式

$$b_{ij}=b_{ij}^{(0)}+b_{ij}^{(1)}x+b_{ij}^{(2)}x^2+\cdots+b_{ij}^{(n-1)}x^{n-1},\ b_{ij}^{(k)}\in F.$$

令 $$A_k=(b_{ij}^{(k)})_{1\le i,j\le n},\quad k=0,1,2,\cdots,n-1,$$
那么 $A_k(0\leqslant k\leqslant n-1)$ 都是 F 上的 $n\times n$ 矩阵，而
$$\operatorname{adj}(xI-A)=A_0+A_1x+A_2x^2+\cdots+A_{n-1}x^{n-1},$$
于是
$$(xI-A)\operatorname{adj}(xI-A)=-AA_0+(A_0-AA_1)x$$
$$+(A_1-AA_2)x^2+\cdots+(A_{n-2}-AA_{n-1})x^{n-1}+A_{n-1}x^n,$$
$$\operatorname{adj}(xI-A)\cdot(xI-A)=-A_0A+(A_0-A_1A)x$$
$$+(A_1-A_2A)x^2+\cdots+(A_{n-2}-A_{n-1}A)x^{n-1}+A_{n-1}x^n.$$
从(7)式推出
$$AA_k=A_kA,\quad k=0,1,2,\cdots,n-1.\tag{8}$$
将 $x=A$ 代入等式
$$(xI-A)\operatorname{adj}(xI-A)=|xI-A|I,\tag{9}$$
双方应该相等．将 $x=A$ 代入(9)式左方并利用(8)式，得
$$-AA_0+(A_0-AA_1)A+(A_1-AA_2)A^2+\cdots$$
$$+(A_{n-2}-AA_{n-1})A^{n-1}+A_{n-1}A^n=0.$$
因此将 $x=A$ 代入(9)式右方也应该等于零矩阵，这样就得到(6)式．

定理 5 设 A 是域 F 上的 $n\times n$ 矩阵，那么 A 的极小多项式是唯一确定的，而且 A 所适合的 $F[x]$ 中的任一多项式都是 A 的极小多项式的倍式．特别，A 的特征多项式是 A 的极小多项式的倍式．

证．设 $f(x)$ 和 $g(x)$ 都是 A 适合的 $F[x]$ 中非零的次数最低的首项系数为 1 的多项式，那么 $\partial^0 f(x)=\partial^0 g(x)$．显然 A 也适合 $f(x)-g(x)$，而 $\partial^0(f(x)-g(x))<\partial^0 f(x)$，因此一定有 $f(x)-g(x)=0$，即 $f(x)=g(x)$．所以 A 的极小多项式是唯一的．

设 $m(x)$ 是 A 的极小多项式，而 A 也适合 $f(x)$．用 $m(x)$ 去除 $f(x)$ 得到

$$f(x)=q(x)m(x)+r(x),\ \partial^0 r(x)<\partial^0 m(x).$$

将 $x=A$ 代入上式，因 $f(A)=0$, $m(A)=0$，所以

$$r(A)=0.$$

即 A 适合 $r(x)$. 因 $\partial^0 r(x)<\partial^0 m(x)$，而 $m(x)$ 是 A 的极小多项式，所以一定有 $r(x)=0$. 于是

$$f(x)=q(x)m(x).$$

这就说 $f(x)$ 是 $m(x)$ 的倍式.

最后，为了以后的需要，我们证明下面这个定理

定理 6 设 F 是一个域，而 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 F 中 n 个元素，那么行列式

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1\leqslant j<i\leqslant n}(\alpha_i-\alpha_j). \tag{10}$$

右方连乘积是对一切数对 (i, j) $(1\leqslant j<i\leqslant n)$ 求积. (这个行列式叫做 n 阶范德蒙德 (Vandermonde) 行列式.) 特别，范德蒙德行列式不等于 0，当且仅当 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 F 里 n 个两两不同的元素.

证. 我们对 n 用归纳法来证明本定理.

当 $n=2$ 时，

$$\begin{vmatrix} 1 & 1 \\ \alpha_1 & \alpha_2 \end{vmatrix} = \alpha_2-\alpha_1,$$

本定理是对的.

设本定理对于 $n-1$ 成立. 现在来证明本定理对 n 也成立.

将范德蒙德行列式的第 n 行减去第 $n-1$ 行乘以 α_1，再将第 $n-1$ 行减去第 $n-2$ 行乘以 α_1, $\cdots$, 最后将第 2 行减去第

1 行乘以 α_1. 我们得到

$$
\begin{vmatrix}
1 & 1 & \cdots & 1 \\
\alpha_1 & \alpha_2 & \cdots & \alpha_n \\
\alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\
\cdots & \cdots & \cdots & \cdots \\
\alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1}
\end{vmatrix}
$$

$$
=\begin{vmatrix}
1 & 1 & 1 & \cdots & 1 \\
0 & \alpha_2-\alpha_1 & \alpha_3-\alpha_1 & \cdots & \alpha_n-\alpha_1 \\
0 & \alpha_2^2-\alpha_1\alpha_2 & \alpha_3^2-\alpha_1\alpha_3 & \cdots & \alpha_n^2-\alpha_1\alpha_n \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
0 & \alpha_2^{n-1}-\alpha_1\alpha_2^{n-2} & \alpha_3^{n-1}-\alpha_1\alpha_3^{n-2} & \cdots & \alpha_n^{n-1}-\alpha_1\alpha_n^{n-2}
\end{vmatrix}
$$

$$
=\begin{vmatrix}
\alpha_2-\alpha_1 & \alpha_3-\alpha_1 & \cdots & \alpha_n-\alpha_1 \\
\alpha_2^2-\alpha_1\alpha_2 & \alpha_3^2-\alpha_1\alpha_3 & \cdots & \alpha_n^2-\alpha_1\alpha_n \\
\cdots & \cdots & \cdots & \cdots \\
\alpha_2^{n-1}-\alpha_1\alpha_2^{n-2} & \alpha_3^{n-1}-\alpha_1\alpha_3^{n-2} & \cdots & \alpha_n^{n-1}-\alpha_1\alpha_n^{n-2}
\end{vmatrix}
$$

$$
=(\alpha_2-\alpha_1)(\alpha_3-\alpha_1)\cdots(\alpha_n-\alpha_1)\times
$$

$$
\times\begin{vmatrix}
1 & 1 & \cdots & 1 \\
\alpha_2 & \alpha_3 & \cdots & \alpha_n \\
\alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\
\cdots & \cdots & \cdots & \cdots \\
\alpha_2^{n-2} & \alpha_3^{n-2} & \cdots & \alpha_n^{n-2}
\end{vmatrix}, \tag{11}
$$

根据归纳法假设

$$
\begin{vmatrix}
1 & 1 & \cdots & 1 \\
\alpha_2 & \alpha_3 & \cdots & \alpha_n \\
\alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\
\cdots & \cdots & \cdots & \cdots \\
\alpha_2^{n-2} & \alpha_3^{n-2} & \cdots & \alpha_n^{n-2}
\end{vmatrix} = \prod_{2\le j<i\le n}(\alpha_i-\alpha_j), \tag{12}
$$

将(12)式代入(11)式就得到(10)式。

最后，我们来讨论矩阵的行列式秩．为此我们先引进矩阵的子式的定义．

定义 8 设

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

是域 F 上的 $m\times n$ 矩阵．再设 $1\leqslant p\leqslant \min(m, n)$ 而

$$1\leqslant i_1<i_2<\cdots<i_p\leqslant m,$$

$$1\leqslant j_1<j_2<\cdots<j_p\leqslant n.$$

我们把位于 A 的第 i_1, i_2, $\cdots$, 或 i_p 行且位于 A 的第 j_1, j_2, $\cdots$, 或 j_p 列的 p^2 个元素所组成的 $p\times p$ 矩阵的行列式

$$\begin{vmatrix} a_{i_1j_1} & a_{i_1j_2} & \cdots & a_{i_1j_p} \\ a_{i_2j_1} & a_{i_2j_2} & \cdots & a_{i_2j_p} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i_pj_1} & a_{i_pj_2} & \cdots & a_{i_pj_p} \end{vmatrix}$$

叫做 A 的一个 p 阶子式，或详细地说，叫做 A 的第 i_1, i_2, $\cdots$, i_p 行，第 j_1, j_2, $\cdots$, j_p 列的 p 阶子式．

定义 9 设 A 是域 F 上的一个 $m\times n$ 矩阵．如果 A 有一个 r 阶子式 $\neq 0$，而 A 的阶数 $>r$ 的子式都等于 0，那么就说 A 的行列式秩等于 r．

如果 $m\times n$ 矩阵 A 的行列式秩等于 r，那么显然 $0\leqslant r\leqslant \min(m, n)$．又如果 A 中 s 阶子式都等于 0，那么根据性质 6，A 中 $s+1$ 阶子式都等于 0，仍根据性质 6，A 中 $s+2$ 阶子式都等于 0，如此继续下去可知 A 中阶数 $>s$ 的子式都等于 0．因此，A 的行列式秩等于 r，当且仅当 A 有一个 r 阶子式 $\neq 0$，而 A 的一切 $r+1$ 阶子式都等于 0．

根据行列式的性质 2，3，4 可知，对 A 的行进行三种初

等变换都不改变 A 的行列式秩，同样根据行列式的性质 $2'$，$3'$，$4'$ 可知，对 A 的列进行三种初等变换也不改变 A 的行列式秩．再设 A 的秩等于 r，那么根据 §2 定理 5，A 一定行等价于 §2 形状 (5) 的一个矩阵 A_0，它的后 $n-r$ 行的元素都是 0，而它的前 r 行中从左往右数第一个非零元素都是 1，这 r 个 1 分属于 r 个不同的列，设它们是第 $k_1, k_2, \cdots, k_r$ 列．显然 A_0 的第 $1, 2, \cdots, r$ 行，第 $k_1, k_2, \cdots, k_r$ 列的 r 阶子式等于 1，而 A_0 的所有 $r+1$ 阶子式都等于 0，因此 A_0 的行列式秩等于 r．更因为作用在 A 的行上的初等变换既不改变 A 的秩也不改变 A 的行列式秩．因此有

定理 7 设 A 是域 F 上的矩阵，那么 A 的秩一定等于 A 的行列式秩．

§6 多项式矩阵

在下一节里，我们将要讨论矩阵在相似变换下的标准形．作为准备，我们在这一节里先讨论一下多项式矩阵．

以前我们所讨论的矩阵的元素都属于某一个域，这种矩阵也叫域上的矩阵，而所谓多项式矩阵是指元素属于一域 F 上的一个文字 x 的多项式环 $F[x]$ 中的矩阵，例如

$$\begin{pmatrix} x^4+x & x^2 & 1 \\ x^3+x+1 & x+1 & -x+2 \end{pmatrix}$$

和

$$\begin{pmatrix} x^5 & x^4 & x+1 \\ x^2+1 & x^3+2 & x^2+5 \\ 2x+1 & 2x^3+5 & 7x^2-x \end{pmatrix}$$

都是多项式矩阵，多项式矩阵也叫多项式环 $F[x]$ 上的矩阵．

$F[x]$ 上的一个 $n\times n$ 矩阵 A 叫做可逆矩阵，如果有 $F[x]$

上的一个 $n\times n$ 矩阵 B 存在，使

$$AB=BA=I^{(n)}$$

成立．这时 B 叫 A 的一个逆矩阵．仿照 § 3 可证，可逆矩阵的逆矩阵是唯一确定的，我们把可逆矩阵 A 的逆记作 A^{-1}．

对于多项式矩阵也可以引进初等矩阵，我们把下面三种形状的 $n\times n$ 多项式矩阵分别叫做第一种、第二种和第三种初等矩阵，它们是：

i) $$D_i(c)=\begin{pmatrix} 1 &&&&&& \\ & 1 &&&&& \\ && \ddots &&&& \\ &&& 1 &&& \\ &&&& c && \\ &&&&& 1 & \\ &&&&&& \ddots \\ &&&&&&& 1 \end{pmatrix}\text{第 } i \text{ 行}$$

（c 位于第 i 列）

这是一个对角矩阵，主对角线上除 (i, i) 位置元素是域 F 中的一个非零元素 c 外，其余元素都是 1．

ii) $$P_{ij}=\begin{pmatrix} 1 &&&&&&&& \\ & \ddots &&&&&&& \\ && 1 &&&&&& \\ &&& 0 && 1 &&& \\ &&&& 1 &&&& \\ &&&&& \ddots &&& \\ &&&&&& 1 && \\ &&& 1 &&& 0 && \\ &&&&&&& 1 & \\ &&&&&&&& \ddots \\ &&&&&&&&& 1 \end{pmatrix}\begin{matrix} \\ \\ \\ \text{第 } i \text{ 行} \\ \\ \\ \\ \text{第 } j \text{ 行} \\ \\ \\ \\ \end{matrix}$$

（第 i 列　第 j 列）

iii) $T_{ij}(d(x))$

$$
=\begin{pmatrix}
1 & & & & & & \\
& 1 & & & & & \\
& & \ddots & & & & \\
& & & 1 & d(x) & & \\
& & & & \ddots & & \\
& & & & & 1 & \\
& & & & & & \ddots \\
& & & & & & & 1
\end{pmatrix}
\begin{matrix} \\ \\ \\ \text{第 } i \text{ 行} \\ \\ \text{第 } j \text{ 行} \\ \\ \\ \end{matrix}
,\quad d(x)\in F[x].
$$

第 i 列　第 j 列

显然初等矩阵都是可逆矩阵，而且它们的逆也都是初等矩阵. 事实上

$$D_i(c)^{-1}=D_i(c^{-1}),\text{ 如果 } c\in F \text{ 而 } c\neq 0.$$

$$P_{ij}{}^{-1}=P_{ij}$$

$$T_{ij}(d(x))^{-1}=T_{ij}(-d(x)),\text{ 其中 } d(x)\in F[x].$$

我们来研究将一个 $m\times n$ 多项式矩阵 A 从前面或后面乘以初等矩阵所引起的作用. 首先，将 A 从前面乘一个第一种 $m\times m$ 初等矩阵 $D_i(c)$ $(c\in F$ 而 $c\neq 0)$ 所引起的作用是将 A 的第 i 行乘以 c, 反之, 将 A 的第 i 行乘以 c $(c\in F$ 而 $c\neq 0)$ 可通过从前面乘以 $D_i(c)$ 来实现. 将 A 从前面乘一个第二种 $m\times m$ 初等矩阵 P_{ij} $(i\neq j)$ 所引起的作用是将 A 的第 i 行和第 j 行互换; 反之将 A 的第 i 行和第 j 行互换可通过从前面乘以 P_{ij} 来实现. 将 A 从前面乘以一个第三种 $m\times m$ 初等矩阵 $T_{ij}(d(x))$ $(i\neq j,\ d(x)\in F[x])$ 所引起的作用是将 A 的第 i 行加上它的第 j 行的 $d(x)$ 倍; 反之将 A 的第 i 行加上它的第 j 行的 $d(x)$ 倍也可以通过将 A 从前面乘以 $T_{ij}(d(x))$ 来实现. 如果将 A 从后面乘以 $n\times n$ 初等矩阵 $D_i(c)$, P_{ij} 或 $T_{ij}(d(x))$ 则引起 A 的列的相应的变换. 将 A 从前面乘以 $m\times m$ 初等矩阵 $D_i(c)$, P_{ij} 或 $T_{ij}(d(x))$ 所引起的 A 的行的变换分别叫做 A

的行的第一种、第二种或第三种初等变换、将 A 从后面乘以 $n\times n$ 初等矩阵 $D_i(c)$，P_{ij} 或 $T_{ij}(d(x))$ 所引起的 A 的列的变换分别叫做 A 的列的第一种、第二种或第三种初等变换.

对于 $F[x]$ 上的 $n\times n$ 矩阵 A 也可以按照 §5 定义 2 来定义它的行列式，也把它记作 $|A|$. §5 中所列举的域 F 上的矩阵的行列式的性质 1–7 和 1′–6′ 对于 $F[x]$ 上的矩阵也成立. §5 中的定理 1 对于 $F[x]$ 上的矩阵同样成立，但 §5 的定理 2 应改述成：

定理 1 设 A 是 $F[x]$ 上的 $n\times n$ 矩阵，那么 A 是可逆矩阵，当且仅当 $|A|$ 是 F 中的非零元素.

这个定理的证明和 §5 定理 2 的证明完全一样，因而略去.

我们也可以平行于 §5 定义 8 和定义 9 来定义 $F[x]$ 上的 $m\times n$ 矩阵 A 的 p 阶子式以及 A 的行列式秩. 和 §5 中一样，可以从行列式的性质 2, 3, 4 及 2′, 3′, 4′ 推出 $F[x]$ 上 $m\times n$ 矩阵 A 的行列式秩在作用在 A 的行的初等变换下不改变，在作用在 A 的列的初等变换下也不改变. 这些我们就都不重复了.

定义 1 $F[x]$ 上两个 $m\times n$ 矩阵叫做等价，如果对一个矩阵的行和列行使有限次初等变换之后可以将它化为另一个矩阵.

我们要研究多项式矩阵在等价下可以化成怎样简单的形状. 我们先给出下面这个定义.

定义 2 设 A 是 $F[x]$ 上的一个 $m\times n$ 矩阵. 再设 $1\leqslant r\leqslant\min(m, n)$. 如果 A 中有一个 r 阶子式不等于 0，就用 $D_r(A)$ 表示 A 中一切 r 阶子式的最高公因式（注意，根据第一章 §2 中的约定，$D_r(A)$ 是首项系数 $=1$ 的多项式）；如果 A 中任一 r 阶子式都等于 0，就规定 $D_r(A)=0$. 我们把 $D_r(A)$ 叫

做 A 的 r 阶行列式因子，而 $\{D_1(A), D_2(A), \cdots, D_{\min(m,n)}(A)\}$ 叫做 A 的行列式因子组. 从行列式的性质 2, 3, 4 及 2′, 3′, 4′ 推出，如果多项式矩阵 A 的行(或列)经过一个行(或列)初等变换变到了 B，那么 A 的一个子式与 B 中同样位置的子式顶多相差 F 中的一个非零因子. 由此即推出

定理 2 等价矩阵的行列式因子组一定相同；即如果 A 和 B 是等价的 $m\times n$ 矩阵，那么

$$D_i(A)=D_i(B),\ 1\leqslant i\leqslant\min(m,n).$$

另一方面，从行列式的性质 6 推出

$$D_i(A)\,|\,D_{i+1}(A),\quad 1\leqslant i\leqslant\min(m,n)-1.$$

我们有

定义 3 设 $F[x]$ 上的 $m\times n$ 矩阵 A 的行列式秩等于 r. 令

$$i_1(A)=D_1(A),\ i_2(A)=\frac{D_2(A)}{D_1(A)},\ \cdots,\ i_r(A)=\frac{D_r(A)}{D_{r-1}(A)}.$$

我们把 $i_1(A), i_2(A), \cdots, i_r(A)$ 叫做 A 的不变因子，而 $\{i_1(A), i_2(A), \cdots, i_r(A)\}$ 叫做 A 的不变因子组.

注意，不变因子都是首项系数等于 1 的多项式.

显然有

定理 3 等价矩阵的不变因子组一定相同.

定理 4 设 A 是 $F[x]$ 上的 $m\times n$ 矩阵，而 A 的秩等于 r. 那么 A 一定等价于对角矩阵

$$\begin{pmatrix} i_1(A) & & & & & \\ & i_2(A) & & & & \\ & & \ddots & & & \\ & & & i_r(A) & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}, \tag{1}$$

其中 $i_1(A), i_2(A), \cdots, i_r(A)$ 是 A 的不变因子，而且

$$i_k(A) \mid i_{k+1}(A), \quad 1 \leqslant k \leqslant r-1.$$

证. 先对 $\min(m, n)$ 用归纳法来证明下面这个断言：A 一定等价于一个对角矩阵

$$\begin{pmatrix} a_1(x) & & & & & \\ & a_2(x) & & & & \\ & & \ddots & & & \\ & & & a_r(x) & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}, \tag{2}$$

其中 $a_k(x)$ 是首项系数为 1 的多项式而

$$a_k(x) \mid a_{k+1}(x), \quad 1 \leqslant k \leqslant r-1$$

只要能够证明，经行和列的初等变换后 A 可化为形状

$$\begin{pmatrix} a_1(x) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{pmatrix}, \tag{3}$$

其中 $a_1(x)$ 是首项系数为 1 的多项式而 $a_1(x)$ 除得尽 A_1 中任一元素即可. 实际上，如果 $\min(m, n)=1$，上述断言已得证. 如果 $\min(m, n)>1$，用归纳法假设亦可证明上述断言.

$$A=\begin{pmatrix} a_{11}(x) & a_{12}(x) & \cdots & a_{1n}(x) \\ a_{21}(x) & a_{22}(x) & \cdots & a_{2n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1}(x) & a_{m2}(x) & \cdots & a_{mn}(x) \end{pmatrix}.$$

如果 $A=0$，A 已是形状 (3) 的矩阵. 如果 $A \neq 0$，经行和列的初等变换后可设 $a_{11}(x) \neq 0$. 再对 $\partial^0 a_{11}(x)$ 作归纳法将 A 化成形状 (3). 如果 $\partial^0 a_{11}(x)=0$，即 $a_{11}(x)$ 是 F 中的非零元素，将它记作 a_{11}，那么将 A 的第一行乘以 a_{11}^{-1}，得一矩阵，仍记

作 A，它的 $a_{11}=1$. 将 A 的第一行乘以 $-a_{21}(x)$，又乘以 $-a_{31}(x)$，…，又乘以 $-a_{m1}(x)$ 分别加到 A 的第2行，第3行，…，第m行上去，得到一个矩阵，它的第一列中的元素除 $a_{11}=1$ 外都等于0，再对这个矩阵的列行使类似的初等变换，即可将这个矩阵化成(3).

假定 $\partial^0 a_{11}(x)<l$ 时，可用初等变换将 A 化为形状 (3). 今设 $\partial^0 a_{11}(x)=l$. 设 A 的第一列中有一个元素 $a_{i1}(x)$ 被 $a_{11}(x)$ 除不尽，可设

$$a_{i1}(x)=q(x)a_{11}(x)+r(x),\quad r(x)\neq 0,\quad \partial^0 r(x)<\partial^0 a_{11}(x).$$

那么将 A 的第一行乘以 $-q(x)$ 加到第 i 行去，然后再将如此得到的矩阵的第一行和第 i 行互换，就得到一个矩阵，它的(1, 1)位置的元素是 $r(x)$. 根据归纳法假设，这个矩阵等价于形状(3)的一个矩阵.

如果 A 的第一行中有一个元素被 $a_{11}(x)$ 除不尽，可对 A 的列进行类似的初等变换，这样仍得到同样的结论.

现在设 A 的第一行和第一列中诸元素都被 $a_{11}(x)$ 整除. 那么将 A 的第一行乘以适当的多项式加到其余诸行去，得一矩阵其第一列的元素除 $a_{11}(x)$ 外都等于0. 再将这个矩阵的第一列乘以适当的多项式加到其余诸列去，得一矩阵其第一行的元素除 $a_{11}(x)$ 外都等于0. 将这个矩阵记作 B，于是 B 有形状

$$\begin{pmatrix} a_{11}(x) & 0 & \cdots & 0 \\ 0 & b_{22}(x) & \cdots & b_{2n}(x) \\ \vdots & \cdots & \cdots & \cdots \\ 0 & b_{m2}(x) & \cdots & b_{mn}(x) \end{pmatrix}.$$

如果这个矩阵 B 中所有 $b_{ij}(x)$ 都被 $a_{11}(x)$ 除尽，那么将 B 的第一行乘以 $a_{11}(x)$ 的首项系数的逆元素，即可将 B 化成形状(3)的矩阵. 反之，设 $b_{ij}(x)$不被 $a_{11}(x)$除尽，那么将 B 的第

j 列加到第 1 列去，得到

$$\begin{pmatrix} a_{11}(x) & 0 & \cdots & 0 \\ b_{2j}(x) & b_{22}(x) & \cdots & b_{2n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ b_{mj}(x) & b_{m2}(x) & \cdots & b_{mn}(x) \end{pmatrix}.$$

对于这个矩阵的行进行上面所进行的初等变换，可得一矩阵，其(1, 1)位置的元素的次数$<\partial^0 a_{11}(x)=l$. 根据归纳法假设，这个矩阵一定等价于形状(3)的一个矩阵.

将矩阵(2)记作 A_0，计算 A_0 的行列式因子可得

$$D_1(A_0)=a_1(x),\ D_2(A_0)=a_1(x)a_2(x),\ \cdots,$$
$$D_r(A_0)=a_1(x)a_2(x)\cdots a_r(x).$$

再计算 A_0 的不变因子可得

$$i_1(A_0)=a_1(x),\ i_2(A_0)=a_2(x),\ \cdots,\ i_r(A_0)=a_r(x).$$

但 A 和 A_0 等价，因此它们有相同的不变因子，于是

$$i_1(A)=a_1(x),\ i_2(A)=a_2(x),\ \cdots,\ i_r(A)=a_r(x).$$

更由 $a_k(x)\mid a_{k+1}(x)$，$1\leqslant k\leqslant r-1$，推出 $i_k(A)\mid i_{k+1}(A)$，$1\leqslant k\leqslant r-1$. 这样定理 4 就完全证明了.

由于对角矩阵 (1) 中的 $i_1(A), i_2(A), \cdots, i_r(A)$ 是 A 的不变因子，因此它们由 A 唯一确定，这样(1)就由 A 唯一确定. (1)叫做 A 在等价变换下的标准形.

系理 1 具有相同不变因子组的两个 $m\times n$ 多项式矩阵一定等价.

系理 2 设 A 是 $F[x]$ 上的 $n\times n$ 可逆矩阵. 那么 A 可以表成初等矩阵的乘积.

证. 如 A 可逆，则 $|A|$ 是 F 中的非零元素. 因此

$$D_n(A)=1.$$

因 $D_k(A)\mid D_{k+1}(A)$，$1\leqslant k\leqslant n-1$，所以 $D_k(A)=1$ 对 $k=1, 2, \cdots, n$. 于是 $i_k(A)=1$ 对 $k=1, 2, \cdots, n$. 因此 A 等价于

单位矩阵，即有初等矩阵 $E_1, E_2, \cdots, E_r$ 和 $E_{r+1}, \cdots, E_{r+s}$ 存在使

$$E_1E_2\cdots E_rAE_{r+1}\cdots E_{r+s}=I^{(n)}$$

因此 $$A=E_r^{-1}\cdots E_2^{-1}E_1^{-1}E_{r+s}^{-1}\cdots E_{r+1}^{-1}.$$

更因初等矩阵的逆矩阵仍是初等矩阵，所以 A 可表成初等矩阵的乘积.

再引进初等因子的概念.

定义 4 设 A 是 $F[x]$ 上的 $m\times n$ 矩阵，而 A 的秩等于 r. 将 A 的 r 个不变因子 $i_1(A), i_2(A), \cdots, i_r(A)$ 分解成 $F[x]$ 中不可约多项式的乘积

$$i_1(A)=p_1(x)^{e_{11}}p_2(x)^{e_{21}}\cdots p_s(x)^{e_{s1}},$$

$$i_2(A)=p_1(x)^{e_{12}}p_2(x)^{e_{22}}\cdots p_s(x)^{e_{s2}},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$i_r(A)=p_1(x)^{e_{1r}}p_2(x)^{e_{2r}}\cdots p_s(x)^{e_{sr}},$$

其中 $p_1(x), p_2(x), \cdots, p_s(x)$ 是两两不同的首项系数等于 1 的不可约多项式，$e_{1r}>0, e_{2r}>0, \cdots, e_{sr}>0$ 而

$$0\leqslant e_{11}\leqslant e_{12}\leqslant\cdots\leqslant e_{1r}$$

$$0\leqslant e_{21}\leqslant e_{22}\leqslant\cdots\leqslant e_{2r}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$0\leqslant e_{s1}\leqslant e_{s2}\leqslant\cdots\leqslant e_{sr}.$$

我们把在 $i_1(A), i_2(A), \cdots, i_r(A)$ 的上述分解式中出现的 $p_i(x)$ 的非 0 次幂 $p_i(x)^{e_{ij}}$ 叫做 A 的初等因子，而

$$\{p_i(x)^{e_{ij}} \mid 1\leqslant i\leqslant s,\ 1\leqslant j\leqslant r \text{ 而 } e_{ij}>0\}$$

叫做 A 的初等因子组.

定理 5 $F[x]$ 上两个 $m\times n$ 矩阵等价，当且仅当它们有相同的秩和初等因子组.

证. 显而易见，$F[x]$ 上一个 $m\times n$ 矩阵 A 的不变因子的个数就等于它的秩，而由初等因子的定义，它们由不变因子

所唯一确定. 反过来，如果知道了 A 的秩与初等因子组，也能求出它的不变因子组. 事实上，如果已知 $m\times n$ 矩阵 A 的秩是 r，而它的初等因子组是

$$
\begin{gathered}
p_1(x)^{e_{11}},\ p_1(x)^{e_{12}},\ \cdots,\ p_1(x)_{e_{1r_1}},\\
p_2(x)^{e_{21}},\ p_2(x)^{e_{22}},\ \cdots,\ p_2(x)_{e_{2r_2}},\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
p_s(x)^{e_{s1}},\ p_s(x)^{e_{s2}},\ \cdots,\ p_s(x)^{e_{sr_s}},
\end{gathered}
$$

其中 $e_{i1}\geqslant e_{i2}\geqslant\cdots\geqslant e_{ir_i}>0,\ i=1,\ 2,\ \cdots,\ s.$

那么 $\max(r_1,\ r_2,\ \cdots,\ r_s)\leqslant r$. 如果令 $e_{ij}=0$ 对 $r_i<j\leqslant r$，那么 A 的不变因子就必然是

$$
\begin{gathered}
i_r(A)=p_1(x)^{e_{11}}p_2(x)^{e_{21}}\cdots p_s(x)^{e_{s1}}\\
i_r(A)=p_1(x)^{e_{12}}p_2(x)^{e_{22}}\cdots p_s(x)^{e_{s2}}\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
i_1(A)=p_1(x)^{e_{1r}}p_2(x)^{e_{2r}}\cdots p_s(x)^{e_{sr}}.
\end{gathered}
$$

定理6 设 A 是 $F[x]$ 上的 $m_1\times n_1$ 矩阵，B 是 $F[x]$ 上的 $m_2\times n_2$ 矩阵. 那么 A 的初等因子组和 B 的初等因子组合在一起就构成

$$
\begin{pmatrix} A & 0\\ 0 & B\end{pmatrix} \tag{4}
$$

的初等因子组.

证. 设 $i_1(A),\ i_2(A),\ \cdots,\ i_r(A)$ 是 A 的不变因子，而 $i_1(B),\ i_2(B),\ \cdots,\ i_t(B)$ 是 B 的不变因子，将它们分解成不可约因式的乘积

$$
\begin{gathered}
i_1(A)=p_1(x)^{e_{11}}p_2(x)^{e_{21}}\cdots p_s(x)^{e_{s1}};\\
i_2(A)=p_1(x)^{e_{12}}p_2(x)^{e_{22}}\cdots p_s(x)^{e_{s2}};\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
i_r(A)=p_1(x)^{e_{1r}}p_2(x)^{e_{2r}}\cdots p_s(x)^{e_{sr}};\\
i_1(B)=p_1(x)^{e'_{11}}p_2(x)^{e'_{21}}\cdots p_s(x)^{e'_{s1}}\\
i_2(B)=p_1(x)^{e'_{12}}p_2(x)^{e'_{22}}\cdots p_s(x)^{e'_{s2}}
\end{gathered}
$$

$$i_t(B)=p_1(x)^{e'_{1t}}p_2(x)^{e'_{2t}}\cdots p_s(x)^{e'_{st}}$$

$$0\leqslant e_{i1}\leqslant e_{i2}\leqslant\cdots\leqslant e_{ir},\quad i=1,\ 2,\ \cdots,\ s;$$

$$0\leqslant e'_{j1}\leqslant e'_{j2}\leqslant\cdots\leqslant e'_{jt},\quad j=1,\ 2,\ \cdots,\ s;$$

$p_i(x)^{e_{ij}}(i=1,\ 2,\ \cdots,\ s,\ j=1,\ 2,\ \cdots,\ r)$ 中不等于 1 的（即 $p_i(x)$ 的指数 e_{ij} 不等于 0 的）那些多项式就组成 A 的初等因子组；$p_i(x)^{e'_{ij}}(i=1,\ 2,\ \cdots,\ s,\ j=1,\ 2,\ \cdots,\ t)$ 中不等于 1 的那些多项式就组成 B 的初等因子组.

将 $e_{11},\ e_{12},\ \cdots,\ e_{1r},\ e'_{11},\ e'_{12},\ \cdots,\ e'_{1t}$ 按大小次序排列成

$$0\leqslant e''_{11}\leqslant e''_{12}\leqslant\cdots\leqslant e''_{1r+t}$$

那么与(4)等价的对角矩阵

$$\begin{pmatrix} i_1(A) & & & & & & & & & & & \\ & i_2(A) & & & & & & & & & & \\ & & \ddots & & & & & & & & & \\ & & & i_r(A) & & & & & & & & \\ & & & & 0 & & & & & & & \\ & & & & & \ddots & & & & & & \\ & & & & & & 0 & & & & & \\ & & & & & & & i_1(B) & & & & \\ & & & & & & & & i_2(B) & & & \\ & & & & & & & & & \ddots & & \\ & & & & & & & & & & i_r(B) & & \\ & & & & & & & & & & & 0 & \\ & & & & & & & & & & & & \ddots & \\ & & & & & & & & & & & & & 0 \end{pmatrix}$$

调动行列后，可化为对角矩阵

$$\begin{pmatrix} p_1(x)^{e''_{11}}(*) & & & & & & \\ & p_1(x)^{e''_{12}}(*) & & & & & \\ & & \ddots & & & & \\ & & & p_1(x)^{e''_{1r+t}}(*) & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

其中$(*)$表示与$p_1(x)$互素的多项式，由此推出(4)的行列式因子$D_1(x), D_2(x), \cdots, D_{r+t}(x)$及不变因子$i_1(x), i_2(x), \cdots, i_{r+t}(x)$有以下诸分解式

$$D_1(x)=p_1(x)^{e''_{11}}(*),\ D_2(x)=p_1(x)^{e''_{11}+e''_{12}}(*),\ \cdots,$$
$$D_{r+t}(x)=p_1(x)^{e''_{11}+e''_{12}+\cdots+e''_{1r+t}}(*),$$
$$i_1(x)=p_1(x)^{e''_{11}}(*), i_2(x)=p_1(x)^{e''_{12}}(*),\ \cdots,$$
$$i_{r+t}(x)=p_1(x)^{e''_{1r+t}}(*).$$

因此 $$p_1(x)^{e''_{11}},\ p_1(x)^{e''_{12}},\ \cdots,\ p_1(x)^{e''_{1r+t}}$$
中不等于1的（即$p_1(x)$的指数等于0的）那些多项式都是(4)的初等因子.

同样方法可定出(4)的$p_2(x), \cdots, p_s(x)$的次幂的初等因子，这样定理6就证明了.

最后我们指出，可以把$F[x]$上的矩阵写成系数是F上的矩阵的多项式，例如

$$\begin{pmatrix} x^4+x & x^2 \\ x^3-x+1 & x-1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}x^4+\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}x^3$$
$$+\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}x^2+\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}x+\begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix}.$$

因此我们往往采用记号$P(x)$来表示$F[x]$上的矩阵. 如果把$P(x)$写成

$$P(x)=P_0x^n+P_1x^{n-1}+\cdots+P_n,$$

其中$P_0, P_1, \cdots, P_n$都是F上的矩阵，我们也说P_0是$P(x)$是首项系数，而n是$P(x)$的次数，记作$\partial^0 P(x)$.

平行于$F[x]$中的带余除法，对于$F[x]$上的$n\times n$矩阵，我们也有带余除法.

定理7 （带余除法） 设$A(x)$和$B(x)$是$F[x]$上的两个$n\times n$矩阵，而$B(x)$的首项系数是F上的$n\times n$可逆矩阵，那么$F[x]$有唯一确定的一对$n\times n$矩阵$Q(x)$和$R(x)$具有

下面的性质:

$$A(x)=Q(x)B(x)+R(x),\ \partial^0 R(x)<\partial^0 B(x). \qquad (5)$$

$F[x]$ 上也有唯一确定的一对 $n\times n$ 矩阵 $Q_1(x)$ 和 $R_1(x)$ 具有下面的性质:

$$A(x)=B(x)Q_1(x)+R_1(x),\ \partial^0 R_1(x)<\partial^0 B(x). \qquad (6)$$

这个定理的证明和第一章 §2 定理 1 的证明完全一样，因而不重复写出了.

我们把适合(5)式的 $Q(x)$ 和 $R(x)$ 分别称为用 $B(x)$ 去右除 $A(x)$ 所得的商和余式，而把适合(6)式的 $Q_1(x)$ 和 $R_1(x)$ 分别称为用 $B(x)$ 去左除 $A(x)$ 所得的商和余式.

§7 矩阵的相似

下面这个定理把矩阵的相似这个问题化到多项式矩阵的等价这个问题，而后面这个问题在上一节里在理论上已经解决了.

定理 1 设 A 和 B 都是 F 上的 $n\times n$ 矩阵. 那么 A 和 B 相似当且仅当多项式矩阵

$$xI-A \quad 和 \quad xI-B$$

等价.

证. 如果 A 和 B 相似，即有 F 上的 $n\times n$ 可逆矩阵 P 存在使

$$A=PBP^{-1},$$

那么

$$xI-A=P(xI-B)P^{-1}.$$

P 和 P^{-1} 自然 $F[x]$ 上的可逆矩阵，因此 $xI-A$ 和 $xI-B$ 等价.

反之，设 $xI-A$ 和 $xI-B$ 等价，即有 $F[x]$ 上的可逆矩阵 $P(x)$ 和 $Q(x)$ 存在使

$$xI-A=P(x)(xI-B)Q(x).$$

设 $P(x)$ 的逆是 $M(x)$，那么

$$M(x)(xI-A)=(xI-B)Q(x). \tag{1}$$

将 $M(x)$ 看作是 x 的多项式，而系数是 F 上的矩阵，用 $xI-B$ 左除 $M(x)$ 得

$$M(x)=(xI-B)N(x)+M, \tag{2}$$

其中 $N(x)$ 是 $F[x]$ 上的矩阵，而 M 是 F 上的矩阵. 将 $Q(x)$ 看作 x 的多项式，而系数是 F 上的矩阵，用 $xI-A$ 右除 $Q(x)$ 得

$$Q(x)=L(x)(xI-A)+N, \tag{3}$$

其中 $L(x)$ 是 $F[x]$ 上的矩阵，而 N 是 F 上的矩阵.

将(2)和(3)代入(1)得

$$\begin{aligned}&(xI-B)N(x)(xI-A)+M(xI-A)\\&=(xI-B)L(x)(xI-A)+(xI-B)N.\end{aligned}$$

于是

$$\begin{aligned}&(xI-B)(N(x)-L(x))(xI-A)\\&=(xI-B)N-M(xI-A).\end{aligned}$$

比较上式双方次数可得 $N(x)=L(x)$. 因此

$$M(xI-A)=(xI-B)N.$$

于是 $$M=N \quad 而 \quad MA=BN.$$

现在来证明 $|M|\neq 0$. 将 $P(x)$ 用 $xI-A$ 左除之得

$$P(x)=(xI-A)H(x)+P,$$

其中 $H(x)$ 是 $F[x]$ 上的矩阵，而 P 是 F 上的矩阵. 于是

$$\begin{aligned}I&=M(x)P(x)=M(x)(xI-A)H(x)+M(x)P\\&=(xI-B)Q(x)H(x)+(xI-B)N(x)P+MP\\&=(xI-B)[Q(x)H(x)+N(x)P]+MP\end{aligned}$$

比较双方次数，得 $Q(x)H(x)+N(x)P=0$. 因此

$$I=MP.$$

于是 $|M|\neq 0$. 因此

$$A=M^{-1}BM.$$

定理1证毕.

定义1 设 A 是域 F 上 $n\times n$ 矩阵. 多项式矩阵 $xI-A$ 的行列式因子,不变因子和初等因子分别叫做 A 的行列式因子,不变因子和初等因子.

系理 F 上两个 $n\times n$ 矩阵 A 和 B 相似, 当且仅当它们有相同的不变因子组, 也当且仅当它们有相同的秩和初等因子组.

证. 这是定理1和§6定理4的系理1及定理5的直接推论.

下面我们就利用这个系理写出 F 上 $n\times n$ 矩阵在相似变换下的标准形,首先我们证明

定理2 F 上的 $n\times n$ 矩阵

$$\begin{pmatrix} 0 & & & & -c_n \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -c_2 \\ & & & 1 & -c_1 \end{pmatrix} \tag{4}$$

的前 $n-1$ 个不变因子都等于1, 第 n 个不变因子是

$$f(x)=x^n+c_1x^{n-1}+c_2x^{n-2}+\cdots+c_n.$$

特别, 当 $f(x)$ 是 $F[x]$ 上一个不可约多项式的幂时, (4)的初等因子即是 $f(x)$.

证. 不难算出(4)的行列式因子是

$$D_1=D_2=\cdots=D_{n-1}=1,\ D_n=f(x).$$

由此即推出本定理.

基于§6定理6和本节定理1的系理及定理2,我们有

定理3 设 F 上 $n\times n$ 矩阵 A 的初等因子组是

$$p_i(x)^{e_{ij}},\ j=1,\ 2,\ \cdots,\ r_i,\ i=1,\ 2,\ \cdots,\ s$$

其中 $p_1(x),\ p_2(x),\ \cdots,\ p_s(x)$ 是 s 个两两不同的不可约多项式，而 e_{ij} 是正整数具有性质

$$e_{i1}\geqslant e_{i2}\geqslant\cdots\geqslant e_{ir_i}>0,\ i=1,\ 2,\ \cdots,\ s.$$

那么 A 相似于 F 上的矩阵

$$B=\begin{pmatrix} M_{11} & & & & & & & & & \\ & M_{12} & & & & & & & & \\ & & \ddots & & & & & & & \\ & & & M_{1r_1} & & & & & & \\ & & & & M_{21} & & & & & \\ & & & & & M_{22} & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & M_{2r_2} & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & M_{s1} \\ & & & & & & & & & & M_{s2} \\ & & & & & & & & & & & \ddots \\ & & & & & & & & & & & & M_{sr_s} \end{pmatrix} \quad (5)$$

其中 $M_{ij}(j=1,\ 2,\ \cdots,\ r_i,\ i=1,\ 2,\ \cdots,\ s)$ 是以 $p_i(x)^{e_{ij}}$ 为初等因子的形如(4)的矩阵. 换句话说，如果 $\partial^0 p_i(x)^{e_{ij}}=n_{ij}$，写

$$p_i(x)^{e_{ij}}=x^{n_{ij}}+c_1^{(i,j)}x^{n_{ij}-1}+c_2^{(i,j)}x^{n_{ij}-2}+\cdots+c_{n_{ij}}^{(i,j)},\ c_k^{(i,j)}\in F,$$

那么 M_{ij} 是 $n_{ij}\times n_{ij}$ 矩阵

$$M_{ij}=\begin{pmatrix} 0 & & & & -c_{n_{ij}}^{(i,j)} \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -c_2^{(i,j)} \\ & & & 1 & -c_1^{(i,j)} \end{pmatrix}.$$

形如(5)的矩阵 B 称为矩阵 A 的有理标准形.

我们还有

定理4 设 F 上的 $n\times n$ 矩阵 A 的不等于1的不变因子组是 $\{\varphi_1(x), \varphi_2(x), \cdots, \varphi_k(x)\}$，其中

$$\varphi_i(x) \mid \varphi_{i+1}(x)\ (1\leqslant i\leqslant k-1),$$

那么 A 相似于 F 上的矩阵

$$C=\begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_k \end{pmatrix}, \tag{6}$$

其中 $C_i(i=1, 2, \cdots, k)$ 是以 $\varphi_i(x)$ 为唯一的不等于1的不变因子的形如(4)的矩阵.

证. 设 $\partial^0\varphi_i(x)=n_i$. 那么

$$xI^{(n)}-C=\begin{pmatrix} xI^{(n_1)}-C_1 & & & \\ & xI^{(n_2)}-C_2 & & \\ & & \ddots & \\ & & & xI^{(n_k)}-C_k \end{pmatrix}.$$

根据假设，它等价于对角矩阵

$$\begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & \varphi_1(x) & & & & & & & \\ & & & & 1 & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & 1 & & & & \\ & & & & & & & \varphi_2(x) & & & \\ & & & & & & & & \ddots & & \\ & & & & & & & & & 1 & & \\ & & & & & & & & & & \ddots & & \\ & & & & & & & & & & & 1 & \\ & & & & & & & & & & & & \varphi_k(x) \end{pmatrix},$$

而上面这个矩阵又等价于对角矩阵

$$\begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ & & & & \varphi_1(x) & & \\ & & & & & \varphi_2(x) & \\ & & & & & & \ddots \\ & & & & & & & \varphi_k(x) \end{pmatrix}.$$

因 $\varphi_i(x) \mid \varphi_{i+1}(x)$ $(1 \leqslant i \leqslant k-1)$，所以 $\{\varphi_1(x),\ \varphi_2(x),\ \cdots,\ \varphi_k(x)\}$就是 C 的不等于 1 的不变因子组. 那么根据定理 1 的系理可知 A 和 C 等价.

形如(6)的矩阵 C 有时也叫矩阵 A 的有理标准形. 但我们约定矩阵 A 的有理标准形指的是形如(5)的矩阵.

第三章　伪随机码介绍

伪随机码又称伪随机序列，是一类有着广泛应用的码. 例如，在连续波雷达中可用作测距信号，在遥控系统中可用作遥控信号，在多址通信中可用作地址信号，在数字通信中可用作群同步信号，还可用作噪声源及在保密通信中起加密作用等等. 在这一章里我们着重介绍的是m序列，因为这是最常用的一类伪随机码，而且它的理论也比较完善. 我们先是对线性移位寄存器序列进行了比较详细的讨论，然后从它再引出m序列. 我们着重讨论了m序列的采样和它的伪随机性. 后面我们也介绍了另外的几类伪随机码的定义，同时为了介绍用电子设备产生它们的方法，我们还介绍了线性移位寄存器的综合算法和非线性移位寄存器. 最后我们介绍了线性移位寄存器的一种推广——自律线性时序线路和q元周期序列的几种表示法.

§1　线性移位寄存器和线性移位寄存器序列

先看几个例子.

例 1　下面是一个 4 级线性移位寄存器的框图.

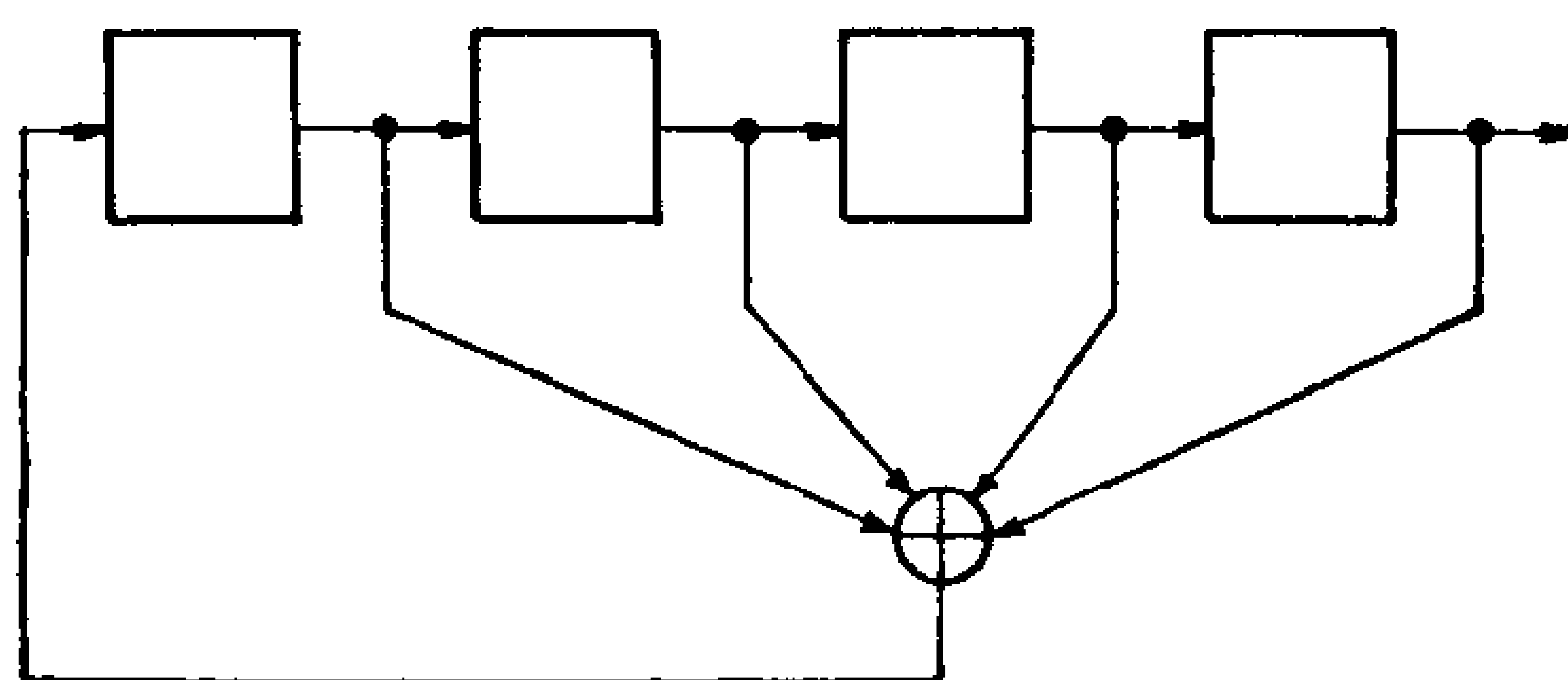


图 1

它由4个寄存器和一个反馈开关电路构成. 图1中的4个小方框代表4个寄存器，从左往右依序叫做第1级、第2级、第3级和第4级寄存器. 每个寄存器可以取0和1这两种状态之一，而0和1总看作是$\mathbf{F}_2$中的元素. 图1中下方的电路图图2代表一个有4个输入端和1个输出端的开关电路，当4个输入端的输入是a_1, a_2, a_3, a_4时，输出端的输出是

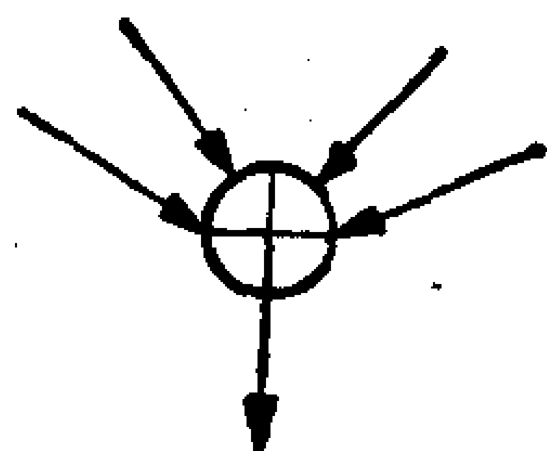


图 2

$$a_1+a_2+a_3+a_4.$$

现在来介绍这个移位寄存器的工作原理. 开始时，设这个移位寄存器的第1级寄存器的内容是a_3，第2级的内容是a_2，第3级的内容是a_1，第4级的内容是a_0，我们就说这个移位寄存器的初始状态是(a_0, a_1, a_2, a_3). 当加上一个移位脉冲时，就将每一级的内容(0或1)移给下一级，最末一级(第4级)的内容就是输出，同时将4个寄存器的内容在$\mathbf{F}_2$中进行加法运算后反馈到第1级去，于是这个4级移位寄存器的状态就成为(a_1, a_2, a_3, a_4)，其中$a_4=a_3+a_2+a_1+a_0$，而输出就是a_0. 再加一个移位脉冲，这个移位寄存器的状态就成为(a_2, a_3, a_4, a_5)，其中$a_5=a_4+a_3+a_2+a_1$，而输出是a_1. 那么不断地加移位脉冲，这个4级移位寄存器的输出就叫做一个移位寄存器序列

$$a_0, a_1, a_2, a_3, \cdots,$$

而这个序列适合递归关系式

$$a_k=a_{k-1}+a_{k-2}+a_{k-3}+a_{k-4}, \quad k\geqslant 4.$$

我们也把这个递归关系式叫做这个移位寄存器的反馈逻辑.

举例来说，设这个移位寄存器的初始状态是(0001)，即第1级的内容是1，第2级、第3级和第4级的内容都是0，那么不断加移位脉冲，这个移位寄存器的输出就是下面这个

序列

$$0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\cdots. \tag{1}$$

这是个周期等于5的序列，即这个序列的6至10项重复1至5项的值，11至15项仍重复1至5项的值，等等.

给上述移位寄存器以初始状态(0011)，那么这个移位寄存器的输出是

$$0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\cdots, \tag{2}$$

这个序列比(1)少1项，即将(1)的第1项略去就得到(2).

类似地，给上述移位寄存器以初始状态(0110)或(1100)或(1000)，那么这个移位寄存器的输出序列分别比(1)少两项或三项或四项.

但是，如果给上述移位寄存器以初始状态(1111)或(0101)，那么分别得到两个全新的序列

$$1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\cdots, \tag{3}$$

$$0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\cdots. \tag{4}$$

它们的周期也都是5. 所谓全新是说它们不能从(1)略去前面某几项得到. 当然也不能从这两个序列中的一个略去前面某几项得到另一个序列.

4级线性移位寄存器总共可以有$2^4=16$个状态，其中(0000)这个状态叫0状态. 如果上述4级移位寄存器的初始状态是0状态(0000)，那么它的输出序列就是0序列

$$0\ 0\ 0\ 0\cdots.$$

容易验证，如果它的初始状态是任意一个非0状态，那么它的输出序列就一定是(1)，或(3)，或(4)，或(1)，(3)，(4)中某一个略去前几项而得到的序列.

这就是说，上述4级线性移位寄存器，由于它的初始状态不同，总共产生四个完全不同的序列：一个是0序列，3个是周期等于5的序列.

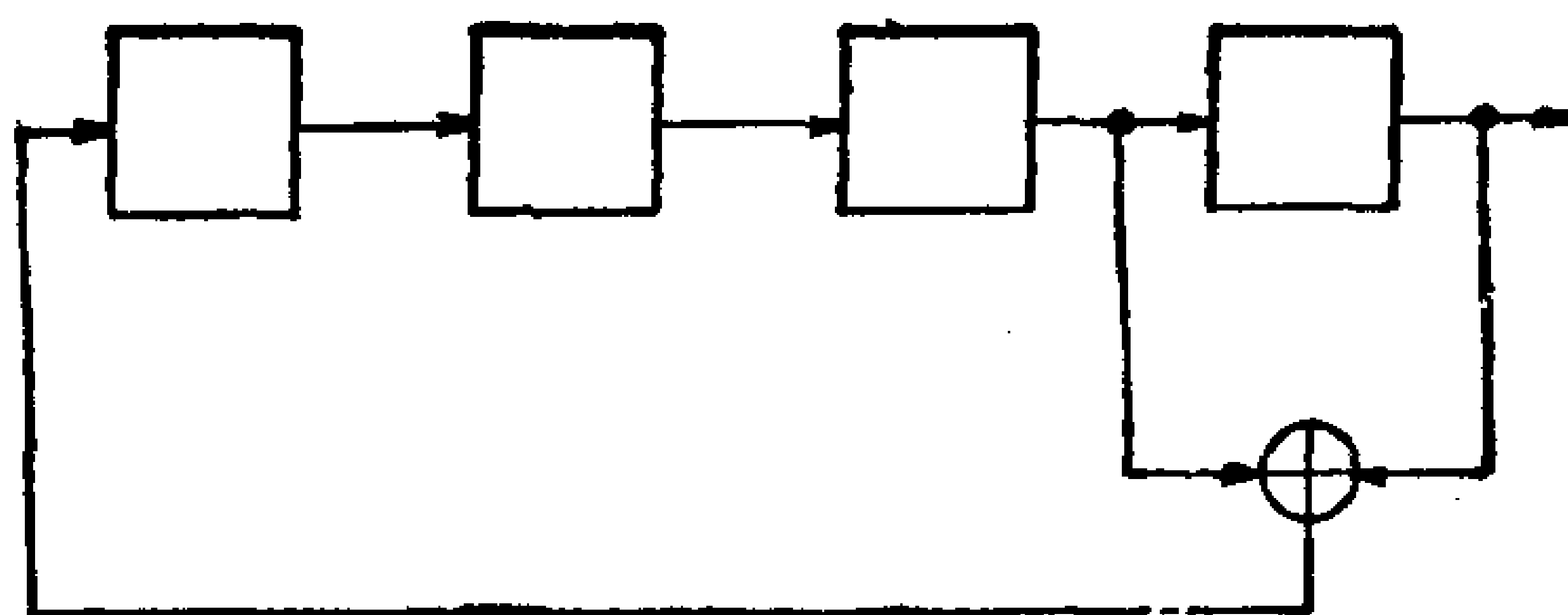


图 3

例 2 再考察一个 4 级线性移位寄存器.

图 3 中电路图

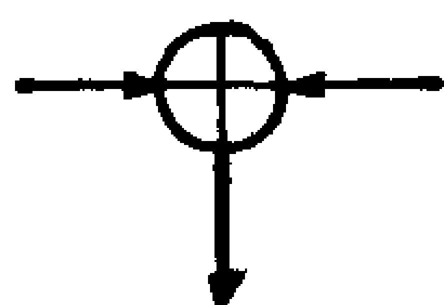


图 4

代表有两个输入端和一个输出端的开关电路，当两个输入端的输入分别是 a_1 和 a_2 时 ($a_1, a_2 \in \mathbf{F}_2$)，输出端的输出就是 $a_1 + a_2$. 这个移位寄存器的反馈逻辑是

$$a_k = a_{k-3} + a_{k-4}, \ k \geqslant 4.$$

给这个移位寄存器以初始状态 (0001)，那么它的输出是个周期等于 15 的序列

$$0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1 \cdots, \tag{5}$$

它的第 16 项至第 30 项分别重复第 1 项至第 15 项的值，等等.

如果这个移位寄存器的初始状态是 0 状态，那么它的输出当然是 0 序列. 但是，如果这个移位寄存器的初始状态是任意一个非 0 状态，那么它的输出序列就是从 (5) 略去前面某几项得到的序列. 例如从初始状态 (1001) 出发，这个移位寄存器产生的序列就是

$$1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0 \cdots,$$

它可以从 (5) 略去前 3 项得到.

这就是说，上述 4 级线性移位寄存器，由于它的初始状态

不同，可以产生两个完全不同的序列：一个是从 0 状态出发产生的 0 序列，一个是从 15 个非 0 状态中的任意一个出发产生的序列.

例 3 再考察另一个 4 级线性移位寄存器.

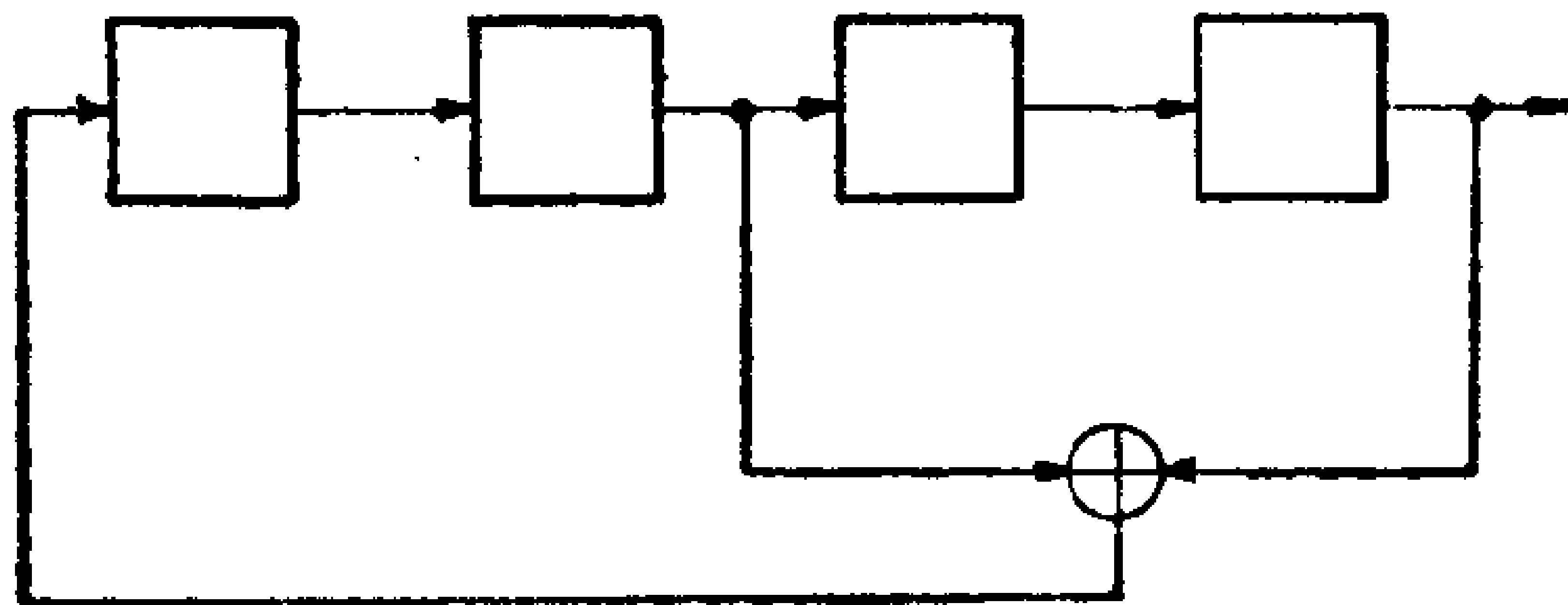


图 5

它的反馈逻辑是

$$a_k = a_{k-2} + a_{k-4},\ k \geqslant 4.$$

除了从 0 状态出发，这个移位寄存器产生 0 序列外，选择不同的非 0 状态作为初始状态，总共可以得到三个完全不同的序列

$$1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0 \cdots,$$

$$0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 1 \cdots,$$

$$1\ 0\ 1\ 1\ 0\ 1 \cdots,$$

它们的周期分别是 6, 6, 3.

现在我们来考察 n 级线性移位寄存器. 下面是一个 n 级线性移位寄存器的框图.

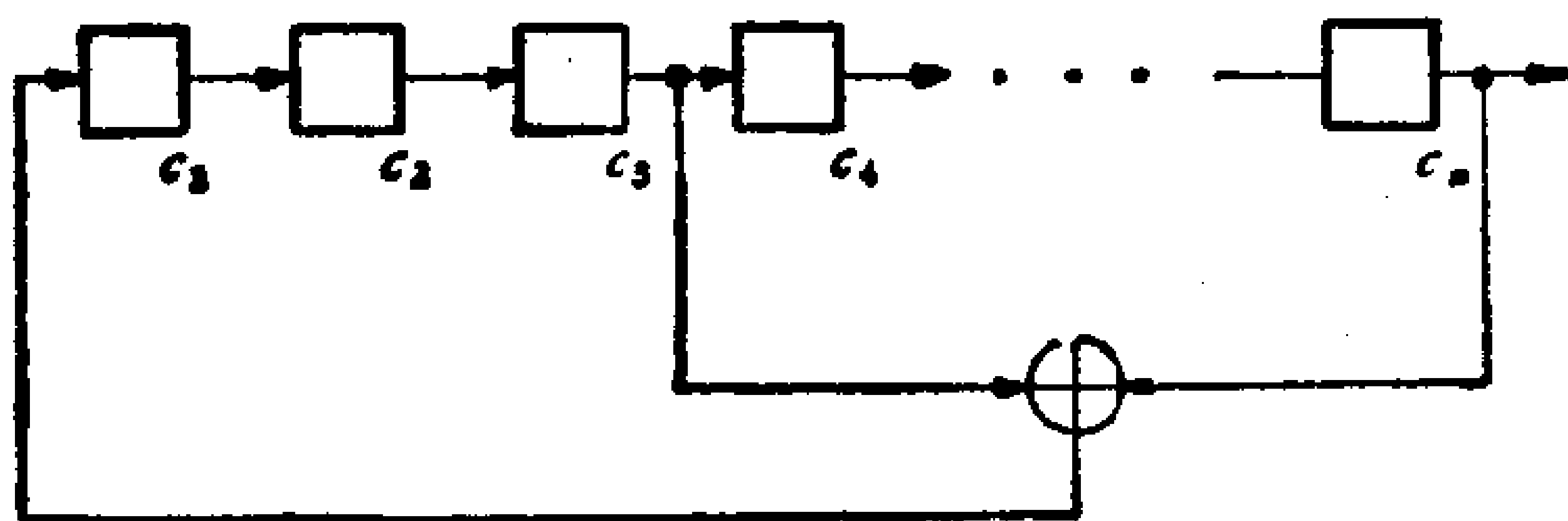


图 6

一个 n 级线性移位寄存器由 n 个寄存器和一个反馈开关电路构成. 每个寄存器的两种状态分别用 0 和 1 来代表，而

0和1总看作是两个元素的有限域$\mathbf{F}_2$中的元素．当加上一个移位脉冲时，就将每级的内容(0或1)移给下一级，最末一级(第n级)移出的内容就是输出．为了保持连续工作，将移位寄存器的某些级的内容在$\mathbf{F}_2$中进行加法运算（即模2加法）后，反馈到第1级去．例如，当第1级的内容为a_{n-1}，第2级的内容为a_{n-2}，…，第n级的内容为a_0给定后，可令

$$a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_na_0$$

反馈到第1级去，其中c_1，c_2，…，c_n都是$\mathbf{F}_2$中的元素，$c_i=0$或1视在$\mathbf{F}_2$中作加法时，不取或取第i级的内容而定．这样，加上一个移位脉冲之后，第1级的内容成为

$$a_n=\sum_{i=1}^{n}c_ia_{n-i},$$

第2级的内容成为a_{n-1}，…，第n级的内容成为a_1，而输出为a_0．于是当给定n级线性移位寄存器的一个初始状态之后，譬如给定第1级的内容为a_{n-1}，第2级的内容为a_{n-2}，…，第n级的内容为a_0，那么不断地加移位脉冲，上述n级线性移位寄存器的输出就成一序列

$$a_0,\ a_1,\ a_2,\ \cdots \tag{6}$$

而这个序列适合线性递归关系式(或反馈逻辑)

$$a_k=\sum_{i=1}^{n}c_ia_{k-i},\quad k\geqslant n. \tag{7}$$

这个序列就叫做n级线性移位寄存器序列．它之所以叫做线性的，是因为递归关系式(7)对于(6)来说是线性的，即反馈逻辑是线性的．

线性移位寄存器和线性移位寄存器序列的概念显然可以推广到q元域$\mathbf{F}_q$上去．形式地用符号

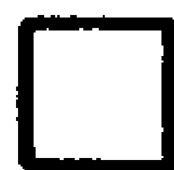


图 7

来代表可以以 q 个状态之一作为状态的一个寄存器，而这 q 个状态分别看作 $\mathbf{F}_q$ 中的 q 个元素．用符号



图 8

来代表一个乘法器，它是当输入是 a 时，输出是 $c \cdot a$ 的开关电路，这里 $c, a \in \mathbf{F}_q$．再用符号

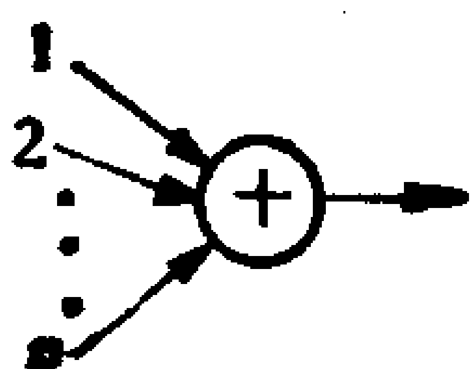


图 9

代表一个加法器，它是有 n 个输入端和一个输出端的开关电路，当 n 个输入端的输入是 $a_1, a_2, \cdots, a_n$ 时 $(a_i \in \mathbf{F}_q)$，那么输出端的输出就是 $a_1+a_2+\cdots+a_n$．这样，下面就是一个 q 元 n 级线性移位寄存器的框图：

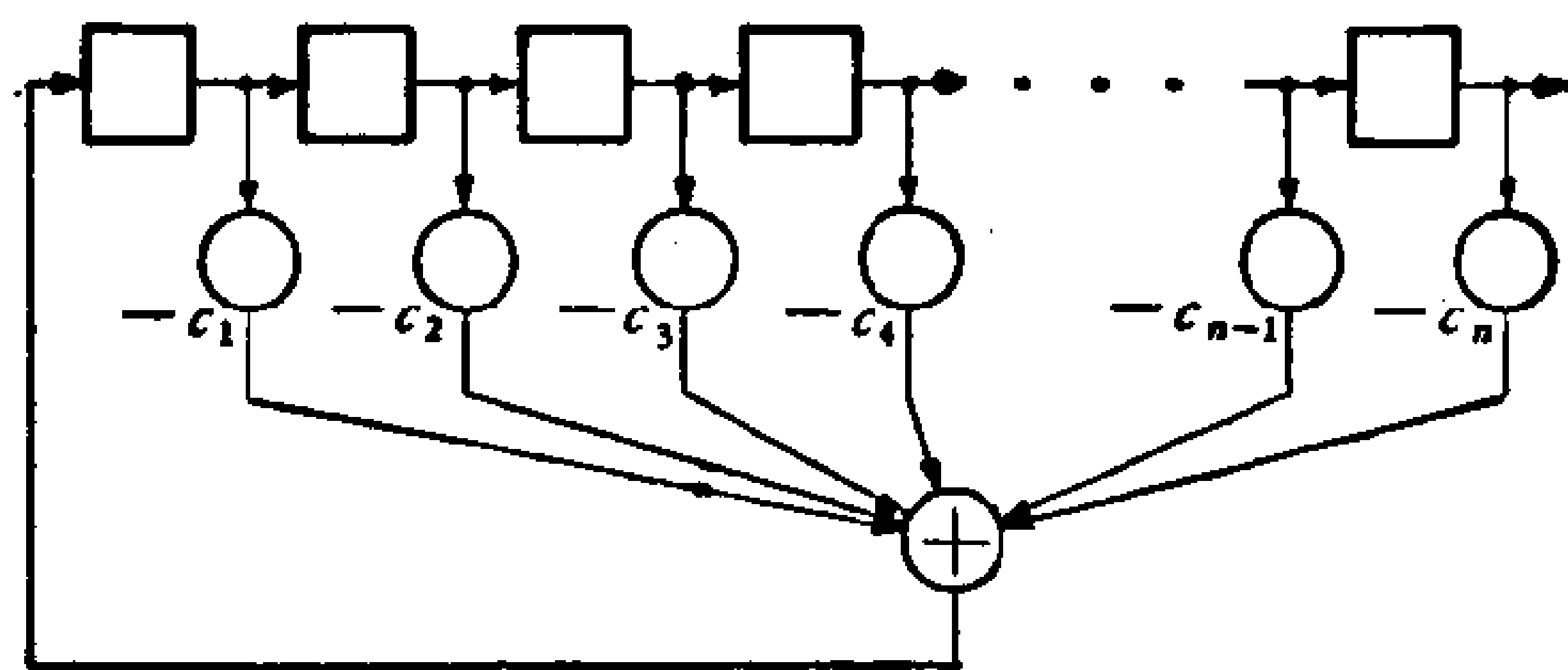


图 10

图中 n 个小方框是 n 个寄存器，把它们从左到右依序叫做第 1 级、第 2 级、…第 n 级寄存器．开始时，设第 1 级的内容是 a_{n-1}，第 2 级的内容是 $a_{n-2}, \cdots$，第 n 级的内容是 a_0，我们就说这个移位寄存器的初始状态是 $(a_0, a_1, \cdots, a_{n-1})$．当加上一个移位脉冲时，就将每一级的内容移给下一级，最末一级

(第 n 级)移出的内容就是输出，同时将各级的内容送给相应的乘法器，而将加法器的输出

$$a_n = -(c_1a_{n-1}+c_2a_{n-2}+\cdots+c_na_0)$$

反馈到第1级去．这样这个移位寄存器的状态就是 $(a_1, a_2, \cdots, a_{n-1}, a_n)$，而输出是 a_0．不断地加移位脉冲，上述 n 级 q 元线性移位寄存器的输出就是一个 q 元序列

$$a_0, a_1, a_2, \cdots, \tag{8}$$

而这个序列适合线性递归关系式(或反馈逻辑)

$$a_k = -\sum_{i=1}^{n} c_ia_{k-i}, \quad k \geqslant n, \tag{9}$$

这个序列就叫做上述 q 元 n 级线性移位寄存器所产生的 q 元 n 级线性移位寄存器序列，简称 q 元 n 级线性移位寄存器序列．它之所以叫线性的，是因为递归关系式(9)对于(8)来说是线性的．

显然 q 元 n 级线性移位寄存器序列(8)由它的前 n 项 $a_0, a_1, \cdots, a_{n-1}$，即它的初始状态 $(a_0, a_1, \cdots, a_{n-1})$ 和递归关系式(9)完全确定．

当然也可以脱离线性移位寄存器来定义线性移位寄存器序列．我们说，q 元序列 (8) 是由线性递归关系式 (9) 产生的 q 元 n 级线性移位寄存器序列，如果它适合递归关系式(9)．

当 $c_n=0$ 时，即当第 n 级寄存器的内容不参加反馈时，可将此 q 元 n 级线性移位寄存器的第 $n-1$ 级的输出看作此移位寄存器的输出，并将序列(1)的首项 a_0 略去，这样剩下的序列

$$a_1, a_2, a_3, \cdots$$

就是一个 $n-1$ 级线性移位寄存器序列．因此当 $c_n=0$ 时，我们就说这个 n 级线性移位寄存器退化成一个 $n-1$ 级线性移

位寄存器，或简单说这个 n 级线性移位寄存器是退化的．而当 $c_n\neq0$ 时，我们就说这个 n 级线性移位寄存器是非退化的．非退化的 n 级线性移位寄存器产生的序列叫非退化的 n 级线性移位寄存器序列．

为了讨论 q 元 n 级线性移位寄存器序列，引进 q 元 n 级线性移位寄存器的联接多项式是方便的．图 5 中的 q 元 n 级线性移位寄存器的联接多项式是

$$f(x)=1+c_1x+c_2x^2+\cdots+c_nx^n. \tag{10}$$

例如，例 1、例 2 和例 3 中的 2 元 4 级线性移位寄存器的联接多项式分别是

$$1+x+x^2+x^3+x^4,\ 1+x^3+x^4,\ 1+x^2+x^4.$$

显然 (10) 由递归关系式 (9) 完全确定．反过来，递归关系式(9)也由联接多项式 (10) 完全确定．因此 q 元 n 级线性移位寄存器序列 (8) 也可以由它的前 n 项 $a_0,\ a_1,\ \cdots,\ a_{n-1}$ 和联接多项式 (10) 完全确定．我们也把适合递归关系式 (9) 的 q 元 n 级线性移位寄存器序列叫做由 $f(x)$ 产生的 q 元 n 级线性移位寄存器序列，简称由 $f(x)$ 产生的序列．我们也常用符号 $G(f)$ 来代表适合线性递归关系式 (9) 的 q 元 n 级线性移位寄存器序列的全体所组成的集合．显然 0 序列属于 $G(f)$，以 0 状态为初始状态就产生 0 序列．$G(f)$ 中其余的序列都是非 0 序列．

我们把适合线性递归关系式 (9) 的 q 元 n 级线性移位寄存器序列 (8) 中的连续 n 个项，如

$$(a_k,\ a_{k+1},\ \cdots,\ a_{k+(n-1)}),\quad k\geqslant0$$

叫做一个状态，记作 $\mathbf{s}_k$，即

$$\mathbf{s}_k=(a_k,\ a_{k+1},\ \cdots,\ a_{k+(n-1)}),\ k\geqslant0.$$

$\mathbf{s}_k$ 可以看作是 $\mathbf{F}_q$ 上的 n 维行向量．将 $\mathbf{s}_k$ 右乘以矩阵

$$
T=\begin{pmatrix}
0 & & & & -c_n \\
1 & 0 & & & -c_{n-1} \\
 & 1 & \ddots & & \vdots \\
 & & \ddots & 0 & -c_2 \\
 & & & 1 & -c_1
\end{pmatrix} \tag{11}
$$

(也说经线性变换T的作用)之后,得到下一状态

$$\mathbf{s}_{k+1}=(a_{k+1},\ a_{k+2},\ \cdots,\ a_{k+n}),$$

而a_{k+n}由递归关系式(9)所确定. 因此q元n级线性移位寄存器序列(8), 由它的初始状态$\mathbf{s}_0=(a_0,\ a_1,\ \cdots,\ a_{n-1})$和$T$完全确定. 我们把$T$叫做由线性递归关系式(9)所确定的变换矩阵, 也叫以(9)为反馈逻辑的线性移位寄存器的状态转移矩阵.

因q元n级线性移位寄存器的初始状态$(a_0,\ a_1,\ \cdots,\ a_n)$中的每一个$a_i$可独立地取$\mathbf{F}_q$中的$q$个元素为值, 所以初始状态一共有$q^n$个可能. 由此推出适合线性递归关系式(9)的$q$元$n$级线性移位寄存器序列的总数是$q^n$.

更进一步, 设

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$
$$\mathbf{b}=(b_0,\ b_1,\ b_2,\ \cdots)$$

是适合线性递归关系式(9)的两个q元n级线性移位寄存器序列. 即

$$a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\ k\geqslant n,$$
$$b_k+c_1b_{k-1}+c_2b_{k-2}+\cdots+c_nb_{k-n}=0,\ k\geqslant n.$$

将以上二式相加得

$$(a_k+b_k)+c_1(a_{k-1}+b_{k-1})+\cdots+c_n(a_{k-n}+b_{k-n})$$
$$=0,\ k\geqslant n.$$

这就是说, 如果定义

$$\mathbf{a}+\mathbf{b}=(a_0+b_0,\ a_1+b_1,\ a_2+b_2,\ \cdots), \tag{12}$$

那么 $\mathbf{a}+\mathbf{b}$ 也是适合线性递归关系式 (9) 的 q 元 n 级线性移位寄存器序列. 容易验证 $G(f)$ 对于按 (12) 式规定的加法运算来说是一个交换群, 以 0 序列

$$\mathbf{0}=(0,\ 0,\ 0,\ \cdots)$$

为单位元素. 如果如下地规定 $\mathbf{F}_q$ 中元素 c 与 $G(f)$ 中元素的乘积:

$$c\cdot(a_0,\ a_1,\ a_2,\ \cdots)=(ca_0,\ ca_1,\ ca_2,\ \cdots),\ c\in\mathbf{F}_q, \tag{13}$$

那么 $G(f)$ 就可以看成是 $\mathbf{F}_q$ 上的一个向量空间. 更因 $|G(f)|=q^n$, 所以 $G(f)$ 是 $\mathbf{F}_q$ 上的 n 维向量空间.

总结以上的讨论, 我们有

定理 1 设 $f(x)=1+\sum_{i=1}^{n}c_ix^i\in\mathbf{F}_q[x]$, 那么适合线性递归关系式 (9) 的 q 元 n 级线性移位寄存器序列的总数是 q^n, 即由 $f(x)$ 所产生的 q 元 n 级线性移位寄存器序列的总数是 q^n, 也即 $|G(f)|=q^n$. 更进一步, $G(f)$ 可看作 $\mathbf{F}_q$ 上的 n 维向量空间.

如果更假定线性递归关系式 (9) 中的 $c_n\neq 0$, 那么由 (9) 所确定的变换矩阵 T 是非异的. T 的特征多项式是

$$|xI-T|.$$

不难证明

$$|xI-T|=x^n+c_1x^{n-1}+c_2x^{n-2}+\cdots+c_n,$$

因此 $|xI-T|$ 和联接多项式 $f(x)$ 是互反多项式, 即

$$\tilde{f}(x)=|xI-T|, \tag{14}$$

而 $$\tilde{f}(x)=x^nf(x^{-1}),\ f(x)=x^n\tilde{f}(x^{-1}).$$

根据凯莱-哈密顿定理 (即第二章 §5 定理 4), 我们有

$$\tilde{f}(T)=0.$$

现在我们证明下面这个引理, 它是以后关于线性移位寄存器序列讨论的基础.

引理 1 设 T 是矩阵 (11)，那么 T 的特征多项式(14)就是它的极小多项式.

证. 令

$$\mathbf{s}_0=(0,\ 0,\ \cdots,\ 0,\ 1)$$

是 $\mathbf{F}_q$ 上的一个 n 维行向量. 那么

$$\begin{aligned}\mathbf{s}_1&=\mathbf{s}_0T=(0,\ 0,\ \cdots,\ 0,\ 1,\ *),\\ \mathbf{s}_2&=\mathbf{s}_0T^2=(0,\ 0,\ \cdots,\ 1,\ *,\ *),\\ &\cdots,\\ \mathbf{s}_{n-1}&=\mathbf{s}_0T^{n-1}=(1,\ *,\ \cdots,\ *,\ *,\ *),\end{aligned}$$

其中 $*$ 代表 $\mathbf{F}_q$ 中某一元素. 显然 $\mathbf{s}_0,\ \mathbf{s}_1,\ \mathbf{s}_2,\ \cdots,\ \mathbf{s}_{n-1}$ 在 $\mathbf{F}_q$ 上线性无关.

设 $h(x)$ 是 T 的极小多项式，并设 $\partial^0 h(x)=m$. 记

$$h(x)=\sum_{i=0}^{m} h_i x^i,$$

那么 $h_m=1$. 于是 T 适合 $h(x)$，即

$$h_0I+h_1T+h_2T^2+\cdots+h_mT^m=0,$$

那么 $$\mathbf{s}_0(h_0I+h_1T+h_2T^2+\cdots+h_mT^m)=0,$$

即 $$h_0\mathbf{s}_0+h_1\mathbf{s}_1+h_2\mathbf{s}_2+\cdots+h_m\mathbf{s}_m=0.$$

这是说 $\mathbf{s}_0,\ \mathbf{s}_1,\ \mathbf{s}_2,\ \cdots,\ \mathbf{s}_m$ 在 $\mathbf{F}_q$ 上线性相关. 因此一定有 $m\geqslant n$. 但是另一方面，设 $\bar{f}(x)$ 是 T 的特征多项式，则 $\bar{f}(T)=0$，而 $\partial^0\bar{f}(x)=n$. 因此 T 的极小多项式 $h(x)$ 的次数 $m\leqslant n$. 于是一定有 $m=n$. 因此根据第二章 §5 定理 5，$\bar{f}(x)$ 就是 T 的极小多项式. 这证明了引理 1.

最后我们指出，把线性递归关系式(2)改写成

$$c_0a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\ k\geqslant n,$$

其中 $c_0=1$，有时是方便的. 为了概括更广的情况，有时我们并不假定 $c_0=1$，即 c_0 可以是 $\mathbf{F}_q$ 中任一元素，特别可以是 0. 这样我们就得到 q 元线性递归序列的概念.

设 $c_0,\ c_1,\ c_2,\ \cdots,\ c_n$ 是 $\mathbf{F}_q$ 中任意给定的 q 个元素，用符

号 $G(c_0, c_1, c_2, \cdots, c_n)$ 表示所有适合线性递归关系式

$$c_0a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0, k\geqslant n, \tag{15}$$

的 q 元序列 $\qquad a_0, a_1, a_2, \cdots,$

所组成的集合．我们把 $G(c_0, c_1, c_2, \cdots, c_n)$ 中的序列叫做适合线性递归关系式(15)的 *q 元线性递归序列*．引进多项式

$$g(x)=c_0+c_1x+c_2x^2+\cdots+c_nx^n,$$

显然 $g(x)$ 由递归关系式(15)唯一确定．因此我们把 $g(x)$ 叫做由递归关系式 (15) 所确定的多项式．我们也把 $G(c_0, c_1, c_2, \cdots, c_n)$ 简记作 $G(g)$．

注意，当 $c_0\neq 0$ 时，线性递归关系式(15)可以改写成

$$a_k=-(c_0^{-1}c_1a_{k-1}+c_0^{-1}c_2a_{k-2}+\cdots+c_0^{-1}c_na_{k-n}),\quad k\geqslant n.$$

因此这时 q 元线性递归序列就是 q 元 n 级线性移位寄存器序列．

§2 线性移位寄存器序列的周期性

在上一节里我们举了三个线性移位寄存器作为例子．它们产生的序列都是周期的．下面我们将证明，非退化的线性移位寄存器产生的序列都是周期的．为此我们先给出周期序列的定义．

定义 1 设有 $\mathbf{F}_q$ 上的一个无限序列(简称 q 元序列)

$$\mathbf{a}=(a_0, a_1, a_2, \cdots) \tag{1}$$

(即 $a_i\in\mathbf{F}_q$，对一切 i)．我们说 $\mathbf{a}$ 是*周期序列*，如果有正整数 l 存在，使

$$a_{l+k}=a_k,\ 对一切非负整数\ k. \tag{2}$$

而满足条件(2)的最小正整数叫做 $\mathbf{a}$ 的*周期*，记作 $p(\mathbf{a})$，即

$$p(\mathbf{a})=\min\{l\,|\,a_{l+k}=a_k,\ 对一切非负整数\ k\}.$$

如果 $\mathbf{a}$ 是 $\mathbf{F}_q$ 上周期 $p(\mathbf{a})$ 的周期序列，那么

$$(a_0,\ a_1,\ a_2,\ \cdots,\ a_{p(\mathbf{a})-1})$$

就叫做 $\mathbf{a}$ 的一个周期.

引理 1 设 $\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)$ 是周期为 $p(\mathbf{a})$ 的 q 元周期序列, 并设有正整数 l 存在使(2)成立, 那么一定有$p(\mathbf{a})\,|\,l$.

证. 如果 $p(\mathbf{a})\nmid l$, 那么由带余除法可设

$$l=tp(\mathbf{a})+r,\ 0<r<p(\mathbf{a}).$$

于是(2)可写成

$$a_{tp(\mathbf{a})+r+k}=a_k,\ \text{对一切}\ k\geqslant 0. \tag{3}$$

因 $\mathbf{a}$ 的周期为 $p(\mathbf{a})$, 我们有

$$a_{p(\mathbf{a})+k}=a_k,\ \text{对一切}\ k\geqslant 0. \tag{4}$$

由(3), (4) 可得

$$a_{r+k}=a_k,\ \text{对一切}\ k\geqslant 0.$$

但 $r<p(\mathbf{a})$, 这与 $p(\mathbf{a})$ 是 $\mathbf{a}$ 的周期的假设相矛盾.

现在考察非退化的 q 元 n 级线性移位寄存器序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$

它适合线性递归关系式

$$c_0a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\ k\geqslant n, \tag{5}$$

其中 $c_0c_n\neq 0$. 将此递归关系式确定的变换矩阵记作 T, 而

$$T=\begin{pmatrix} 0 & & & & -c_0^{-1}c_n \\ 1 & 0 & & 0 & -c_0^{-1}c_{n-1} \\ & 1 & \ddots & & \vdots \\ & 0 & \ddots & 0 & -c_0^{-1}c_2 \\ & & & 1 & -c_0^{-1}c_1 \end{pmatrix},$$

那么 T 非异. 再令

$$\mathbf{s}_0=(a_0,\ a_1,\ \cdots,\ a_{n-1}),$$

那么就得到一个状态序列

$$\mathbf{s}_0,\ \mathbf{s}_1=\mathbf{s}_0T,\ \mathbf{s}_2=\mathbf{s}_0T^2,\ \cdots,$$

其中 $\quad \mathbf{s}_k=\mathbf{s}_0T^k=(a_k,\ a_{k+1},\ a_{k+2},\ \cdots,\ a_{k+n-1}),$

$$k=0,\ 1,\ 2,\ \cdots.$$

我们有

引理 2 设 $\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)$ 是适合线性递归关系式 (5) 的非退化的 q 元 n 级线性移位寄存器序列. 如果 $\mathbf{a}$ 是周期为 $p(\mathbf{a})$ 的周期序列, 那么一定有 $\mathbf{s}_0T^{p(\mathbf{a})}=\mathbf{s}_0$, 而且下面这 $p(\mathbf{a})$ 个状态

$$\mathbf{s}_0,\ \mathbf{s}_0T,\ \mathbf{s}_0T^2,\ \cdots,\ \mathbf{s}_0T^{p(\mathbf{a})-1} \tag{6}$$

两两不同. 反之, 如果 l 是最小正整数使 $\mathbf{s}_0T^l=\mathbf{s}_0$, 那么 $\mathbf{a}$ 是周期为 l 的周期序列.

证. 设 $\mathbf{a}$ 是周期为 $p(\mathbf{a})$ 的周期序列, 那么

$$a_{p(\mathbf{a})+k}=a_k,\ \text{对一切非负整数}\ k.$$

因此
$$(a_{p(\mathbf{a})},\ a_{p(\mathbf{a})+1},\ a_{p(\mathbf{a})+2},\ \cdots,\ a_{p(\mathbf{a})+n-1})$$
$$=(a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1}).$$

这就是说
$$\mathbf{s}_0T^{p(\mathbf{a})}=\mathbf{s}_0.$$

更进一步, 设

$$\mathbf{s}_0T^i=\mathbf{s}_0T^j,\ \text{而}\ 0\leqslant i\leqslant j\leqslant p(\mathbf{a})-1.$$

令 $\tau=j-i$. 因 T 非异, 所以有

$$\mathbf{s}_0T^\tau=\mathbf{s}_0,$$

于是 $\mathbf{s}_kT^\tau=\mathbf{s}_0T^kT^\tau=\mathbf{s}_0T^\tau T^k=\mathbf{s}_0T^k=\mathbf{s}_k$, 对一切 $k\geqslant0$.

由此推出
$$a_{\tau+k}=a_k,\ \text{对一切}\ k\geqslant0.$$

根据引理 1 就有 $p(\mathbf{a})\,|\,\tau$. 但 $\tau=j-i\leqslant p(\mathbf{a})-1$. 因此 $\tau=0$, 即 $i=j$. 这证明了 (6) 中 $p(\mathbf{a})$ 个状态两两不同.

反之, 设 l 是最小正整数使 $\mathbf{s}_0T^l=\mathbf{s}_0$, 那么

$$\mathbf{s}_kT^l=\mathbf{s}_k,\ \text{对一切}\ k\geqslant0.$$

由此推出
$$a_{l+k}=a_k,\ \text{对一切}\ k\geqslant0.$$

这就是说 $\mathbf{a}$ 的周期 $p(\mathbf{a})\,|\,l$. 但 $s_0T^{p(\mathbf{a})}=s_0$, 因此 $p(\mathbf{a})\geqslant l$. 所以 $l=p(\mathbf{a})$.

从这个引理可以推出

定理 1 非退化的 q 元 n 级线性移位寄存器序列一定是

周期序列，而且它的周期 $\leqslant q^n-1$.

证. 设 $\mathbf{a}=(a_0, a_1, a_2, \cdots)$

是个非退化的 q 元 n 级线性移位寄存器序列，它适合线性递归关系式 (5). 考察 $\mathbf{a}$ 的状态序列

$$\mathbf{s}_0, \ \mathbf{s}_1=\mathbf{s}_0T, \ \mathbf{s}_2=\mathbf{s}_0T^2, \ \cdots \tag{7}$$

它们都是 $\mathbf{F}_q$ 上的 n 维行向量. 设有某一状态，如 $\mathbf{s}_i=\mathbf{0}=(0, 0, \cdots, 0)$，那么 $\mathbf{s}_{i+1}=\mathbf{s}_iT=\mathbf{0}T=\mathbf{0}$, $\mathbf{s}_{i+2}=\mathbf{s}_{i+1}T=\mathbf{0}T=\mathbf{0}$, $\cdots$, 也有 $\mathbf{s}_{i-1}=\mathbf{s}_iT^{-1}=\mathbf{0}T^{-1}=\mathbf{0}$, $\mathbf{s}_{i-2}=\mathbf{s}_{i-1}T^{-1}=\mathbf{0}T^{-1}=\mathbf{0}$, $\cdots$, $s_0=\mathbf{0}$. 因此 $\mathbf{a}$ 是 $\mathbf{0}$ 序列. 这时 $\mathbf{a}$ 是周期 1 的周期序列. 如果 $\mathbf{a}$ 的状态序列 (7) 中 $\mathbf{0}$ 状态不出现，那么它们就都是 $\mathbf{F}_q$ 上的非零 n 维行向量. 但 $\mathbf{F}_q$ 总共有 q^n-1 个非零 n 维行向量，所以上述状态序列的前 q^n 个状态不能两两相异. 于是有 i, j 存在，$0\leqslant i<j\leqslant q^n-1$, 使

$$\mathbf{s}_0T^i=\mathbf{s}_0T^j.$$

因 T 非异，所以有

$$\mathbf{s}_0T^{j-i}=\mathbf{s}_0.$$

令 l 是最小正整数使

$$\mathbf{s}_0T^l=\mathbf{s}_0,$$

那么 $l\leqslant j-i\leqslant q^n-1$, 而根据引理 2, l 就是 $\mathbf{a}$ 的周期. 这证明了定理 1.

当 n 级线性移位寄存器序列的周期达到极大值 q^n-1 时，它就叫最长 q 元 n 级线性移位寄存器序列，简称 q 元 m 序列，更简称 m 序列. 我们看到 § 1 例 2 中的 4 级线性移位寄存器序列的周期是 15, 而 $15=2^4-1$, 因此这个序列是个二元 m 序列. m 序列是很重要的一类线性移位寄存器序列，将在 § 4—§ 6 中对它进行较详细的讨论. 在本节中我们将先讨论一般的线性移位寄存器序列.

首先我们注意，如果 $\mathbf{a}$ 是周期 l 的周期序列，那么 $\mathbf{a}$ 显然

适合线性递归关系式

$$a_k - a_{k-l} = 0,\ k \geqslant l,$$

而它的联接多项式是

$$1 - x^l,$$

因此周期序列一定是线性移位寄存器序列.更进一步,我们有

定理 2 设 $\mathbf{a}$ 是 $\mathbf{F}_q$ 上的一个周期序列,那么存在着 $\mathbf{F}_q$ 上的一个零次项等于 1 的多项式 $f(x)$ 具有性质: $a \in G(h(x))$,当且仅当 $f(x) \mid h(x)$.更进一步,适合上述性质的多项式 $f(x)$ 是唯一确定的. 如果 $\mathbf{a}$ 是非零周期序列,那么 $\partial^0 f(x) \geqslant 1$.

证. 令 $I = \{h(x) \mid h(x) \in \mathbf{F}_q[x], \text{而} \mathbf{a} \in G(h)\}$.

我们来证明 I 是 $\mathbf{F}_q[x]$ 中的一个非零理想,即含有非零多项式的理想.

首先,设 l 是 $\mathbf{a}$ 的周期,那么 $1 - x^l \in I$. 因此 I 含有非零多项式.

其次,设 $g(x)$, $h(x) \in I$. 写

$$g(x) = \sum_{i=0}^{n} c_i x^i,$$

$$h(x) = \sum_{i=0}^{m} d_i x^i,$$

那么 $$c_0 a_k + c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_n a_{k-n} = 0,\ k \geqslant n,$$

$$d_0 a_k + d_1 a_{k-1} + d_2 a_{k-2} + \cdots + d_m a_{k-m} = 0,\ k \geqslant m.$$

令 $M = \max(n, m)$. 再令

$$c_{n+1} = c_{n+2} = \cdots = c_M = 0,\ \text{如果}\ M > n,$$

$$d_{m+1} = d_{m+2} = \cdots = d_M = 0,\ \text{如果}\ M > m.$$

于是有

$$c_0 a_k + c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_M a_{k-M} = 0,\ k \geqslant M.$$

$$d_0 a_k + d_1 a_{k-1} + d_2 a_{k-2} + \cdots + d_M a_{k-M} = 0,\ k \geqslant M.$$

由上面两个式子推出

$$(c_0-d_0)a_k+(c_1-d_1)a_{k-1}+(c_2-d_2)a_{k-2}+\cdots$$
$$+(c_M-d_M)a_{k-M}=0,\quad k\geqslant M.$$

这个递归关系式所确定的多项式是

$$\sum_{i=0}^{M}(c_i-d_i)x^i=g(x)-h(x).$$

因此 $a\in G(g-h)$. 于是 $g(x)-h(x)\in I$.

再设 $g(x)=\sum_{i=0}^{n}c_ix^i\in I$, 那么有

$$c_0a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\quad k\geqslant n.$$

置 $$d_0=0,\ d_1=c_0,\ d_2=c_1,\ d_3=c_2,\ \cdots,\ d_{n+1}=c_n,$$

那么 $$d_0a_k+d_1a_{k-1}+d_2a_{k-2}+\cdots$$
$$+d_{n+1}a_{k-(n+1)}=0,\quad k\geqslant n+1.$$

这个递归关系式所确定的多项式是

$$\sum_{i=0}^{n+1}d_ix^i=x\sum_{i=1}^{n+1}d_ix^{i-1}=x\sum_{i=1}^{n}c_ix^i=xg(x).$$

因此 $a\in G(xg(x))$. 于是 $xg(x)\in I$. 更进一步, 对 i 用数学归纳法可以证明, 对任意非负整数 i, $x^ig(x)\in I$. 由此推出, 对任意多项式 $\sum_{i=0}^{m}b_ix^i\in\mathbf{F}_q[x]$,

$$\left(\sum_{i=0}^{m}b_ix^i\right)g(x)=\sum_{i=0}^{m}(b_ix^ig(x))\in I.$$

根据第一章 §6定理 4, 我们知道 I 是 $\mathbf{F}_q[x]$ 的一个非零理想. 再根据第一章 §6 定理 6 可知, $\mathbf{F}_q[x]$ 中有一个非零多项式 $f(x)$ 存在, 使 $I=(f(x))$, 即 I 是由被 $f(x)$ 所整除的所有多项式组成的理想. 自然可以设 $f(x)$ 的零次项等于 1. $f(x)$ 显然有性质: $\mathbf{a}\in G(h(x))$, 当且仅当 $f(x)\mid h(x)$.

又假定 $f_1(x)$ 也是 $\mathbf{F}_q[x]$ 中的一个零次项等于 1 的多项式并具有性质: $\mathbf{a}\in G(h(x))$, 当且仅当 $f_1(x)\mid h(x)$. 那么一定有 $f(x)\mid f_1(x)$ 和 $f_1(x)\mid f(x)$. 因此 $f_1(x)=cf(x)$ 而 $c\in\mathbf{F}_q$,

$c\neq 0$. 但 $f(x)$ 和 $f_1(x)$ 的零次项都等于 1, 所以一定有 $c=1$. 因此 $f_1(x)=f(x)$. 这证明了 $f(x)$ 的唯一性.

又当 $\mathbf{a}$ 不是零序列时, 显然有 $\partial^0 f(x)\geqslant 1$.

这样定理 2 就完全证明了.

定义 2 设 $\mathbf{a}$ 是 $\mathbf{F}_q$ 上的一个周期序列, 那么由定理 2 知 $\mathbf{F}_q[x]$ 中有唯一的一个零次项等于 1 的多项式 $f(x)$, 具有性质: $\mathbf{a}\in G(h(x))$, 当且仅当 $f(x)\,|\,h(x)$. 这个多项式 $f(x)$ 叫做 $\mathbf{a}$ 的极小多项式.

有了定义 2, 那么定理 2 是说, 任一周期序列必有一极小多项式, 反过来, 我们有

定理 3 任给 $f(x)$ 是 $\mathbf{F}_q[x]$ 中一个零次项等于 1 的多项式. 那么总有 $\mathbf{F}_q$ 上的一个周期序列存在, 它以 $f(x)$ 为极小多项式. 实际上, 当 $\partial^0 f(x)=n\geqslant 1$ 时, 由以 $f(x)$ 为联接多项式的 q 元 n 级线性移位寄存器, 从初始状态 $(0, 0, \cdots, 0, 1)$ 出发, 所产生的线性移位寄存器序列就以 $f(x)$ 为极小多项式.

证. 设 $\partial^0 f(x)=n$. 当 $n=0$ 时, 零序列就以 $f(x)=1$ 为极小多项式. 以下设 $n>0$. 写

$$f(x)=1+\sum_{i=1}^{n} c_i x^i,$$

那么 $c_n\neq 0$. 考察从初始状态

$$\mathbf{s}_0=(0,\ 0,\ \cdots,\ 0,\ 1)$$

出发的适合递归关系式

$$a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\quad k\geqslant n$$

的 q 元 n 级线性移位寄存器序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$

其中 $a_0=a_1=a_2=\cdots=a_{n-2}=0$, $a_{n-1}=1$. 设 $h(x)$ 是 $\mathbf{a}$ 的极小多项式, 并设 $\partial^0 h(x)=m$. 写

$$h(x)=1+\sum_{i=1}^{m}d_ix^i,$$

那么 $\mathbf{a}$ 适合

$$a_k+d_1a_{k-1}+d_2a_{k-2}+\cdots+d_ma_{k-m}=0,\quad k\geqslant m. \tag{8}$$

根据定理 2, $h(x)\mid f(x)$. 如果 $f(x)$ 不是 $\mathbf{a}$ 的极小多项式, 那么 $\partial^0h(x)<\partial^0f(x)$, 即 $m<n$. 这时 $\mathbf{a}$ 是从 $(a_0, a_1, \cdots, a_{m-1})$ 出发而适合线性递归关系式(8)的线性移位寄存器序列, 因而是零序列. 但 $a_{n-1}=1\neq0$. 这是一个矛盾, 因此 $f(x)$ 是 $\mathbf{a}$ 的极小多项式.

下面我们试图用周期序列的极小多项式来刻划它的周期. 为此我们给出下面这个定义.

定义 3 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个次数 $\geqslant1$ 的而零次项 $\neq0$ 的多项式. 我们定义 $f(x)$ 的周期为最小正整数 l 使 $f(x)\mid x^l-1$. 我们用 $p(f)$ 来表示 $f(x)$ 的周期.

注意, 当 $f(x)$ 是 $\mathbf{F}_q$ 上的不可约多项式时, 这个定义与第一章 §5 定义 2 中所给出的 $\mathbf{F}_q$ 上不可约多项式的周期的定义是一致的. 实际上, 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个 n 次不可约多项式, $f(x)\neq x$, 并设 l 是它按照定义 3 规定的周期, 而 l' 是它按照第一章 §5 定义 2 规定的周期. 那么 l 是最小正整数使 $f(x)\mid x^l-1$. 而 l' 是 $f(x)$ 的 n 个根 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 的公共阶. 从 $f(x)\mid x^l-1$ 推出 $f(x)$ 的根 α_i 都是 x^l-1 的根, 因此 $\alpha_i^l=1$, 于是 $l'\mid l$. 反过来, 我们有 $\alpha_i^{l'}=1$, 即 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 都是 $x^{l'}-1$ 的根. 于是 $(x-\alpha_i)\mid x^{l'}-1$. 因 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 两两相异, 所以

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\mid x^{l'}-1.$$

但 $f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, $a\in\mathbf{F}_q$ 而 $a\neq0$, 所以 $f(x)\mid x^{l'}-1$. 由此推出 $l\leqslant l'$. 从 $l\leqslant l'$ 和 $l'\mid l$ 推出 $l=l'$.

我们回忆一下, 在第一章 §4 例 2 中, 我们曾令

$$\mathbf{F}_q[x]^*_{f(x)}=\{h(x)\,|\,h(x)\in\mathbf{F}_q[x],$$
$$\partial^0 h(x)<\partial^0 f(x) \text{ 而 } (h(x),\, f(x))=1\},$$

并在其中规定了乘法运算

$$h(x)\odot g(x)=(h(x)g(x))_{f(x)},\ \text{对 } h(x),\ g(x)\in\mathbf{F}_q[x]^*_{f(x)}.$$

我们知道 $\mathbf{F}_q[x]^*_{f(x)}$ 是个交换群. 我们可以给出定义 3 的一个等价的定义.

定义 3′ 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个次数 $n\geqslant 1$ 而零次项不等于 0 的多项式. $f(x)$ 的周期就是交换群 $\mathbf{F}_q[x]^*_{f(x)}$ 中元素 x 的阶.

实际上, 设 l 是 $f(x)$ 按定义 3 规定的周期, 而 l' 是它按定义 3′ 规定的周期. 从 $f(x)\,|\,x^l-1$ 推出, 在 $\mathbf{F}_q[x]_{f(x)}$ 中

$$\underbrace{x\odot x\odot\cdots\odot x}_{l\text{个}}-1=(x^l-1)_{f(x)}=0,$$

于是在 $\mathbf{F}_q[x]^*_{f(x)}$ 中

$$\underbrace{x\odot x\odot\cdots\odot x}_{l\text{个}}=1.$$

根据第一章 § 4 定理 4 就有 $l'\,|\,l$. 另一方面, 从

$$\underbrace{x\odot x\odot\cdots\odot x}_{l'\text{个}}=1$$

推出
$$(x^{l'}-1)_{f(x)}=\underbrace{x\odot x\odot\cdots\odot x}_{l'\text{个}}-1=0,$$

即
$$f(x)\,|\,x^{l'}-1.$$

因此 $l\leqslant l'$. 那么从 $l'\,|\,l$ 和 $l\leqslant l'$ 就推出 $l=l'$. 这证明了定义 3 和定义 3′ 是等价的.

从定义 3′ 可以推出

引理 3 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个次数 $n\geqslant 1$ 而零次项不等于 0 的多项式, 并设 $f(x)\,|\,x^l-1$, 那么一定有 $p(f)\,|\,l$.

证. 设 $f(x)\,|\,x^l-1$. 那么在 $\mathbf{F}_q[x]^*_{f(x)}$ 中,

$$x^l = \underbrace{x \odot x \odot \cdots \odot x}_{l\text{个}} = 1,$$

于是根据第一章 § 4 定理 4, $p(f) \mid l$.

我们还有

引理 4 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个零次项不等于 0 的不可约多项式, 那么 $p(f) \mid q^{\partial^0 f(x)} - 1$.

证. 设 $\partial^0 f(x) = n$. 因 $f(x)$ 不可约, $n \geqslant 1$. 但当 $f(x)$ 不可约时, $\mathbf{F}_q[x]_{f(x)}$ 是域, 这时 $\mathbf{F}_q[x]^*_{f(x)}$ 就是 $\mathbf{F}_q[x]_{f(x)}$ 中全体非零元素所组成的乘法群. 因此 $|\mathbf{F}_q[x]^*_{f(x)}| = q^n - 1$. 根据第一章 § 4 定理 5, $\mathbf{F}_q[x]^*_{f(x)}$ 是循环群, 即 $\mathbf{F}_q[x]^*_{f(x)}$ 中有一个 $q^n - 1$ 阶元素 α, 而 $\mathbf{F}_q[x]^*_{f(x)} = [\alpha]$. 特别, $x = \alpha^i$ 而 $0 < i < q^n - 1$. 那么

$$x^{q^n - 1} = (\alpha^i)^{q^n - 1} = (\alpha^{q^n - 1})^i = 1^i = 1.$$

因此 $p(f) \mid q^n - 1$, 即 $p(f) \mid q^{\partial^0 f(x)} - 1$.

定义 4 设 A 是 $\mathbf{F}_q$ 上的一个 $n \times n$ 非异矩阵. 如果有正整数 l 存在使 $A^l = I$, 这里 I 是 $n \times n$ 单位矩阵, A 就叫有限阶矩阵. 如果 A 是有限阶矩阵, 那么适合条件 $A^l = I$ 的最小正整数就叫做 A 的阶. 我们用 $p(A)$ 来表示 A 的阶.

引理 5 设 A 是 $\mathbf{F}_q$ 上的一个 $n \times n$ 非异矩阵, 那么 A 一定是有限阶的. 更进一步, 如果有正整数 l 适合条件 $A^l = I$, 那么 $p(A) \mid l$.

证. 因 $\mathbf{F}_q$ 上 $n \times n$ 矩阵的个数有限, 所以下面这一系列矩阵

$$A^0 = I,\ A^1 = A,\ A^2,\ A^3,\ \cdots$$

不能两两不同. 设

$$A^i = A^j,\ j > i \geqslant 0.$$

因 A 非异, 故 A^{-1} 存在. 将上式双方都乘以 A^{-i} 就有

$$A^{j-i} = I,\ j - i > 0.$$

因此 A 是有限阶的.

更进一步，设 $A^l=I$. 根据带余除法，有

$$l=tp(A)+r,\ 0\leqslant r<p(A).$$

那么 $$I=A^l=A^{tp(A)+r}=A^{tp(A)}\cdot A^r=(A^{p(A)})^t\cdot A^r$$
$$=I^t\cdot A^r=I\cdot A^r=A^r.$$

由 $p(A)$ 的极小性即可推出 $r=0$. 因此 $p(A)\mid l$.

引理 6 设

$$f(x)=1+\sum_{i=1}^{n}c_ix^i\in\mathbf{F}_q[x],$$

并假定 $c_n\neq 0$. 令 T 是§1第 (11) 式中的矩阵，那么 $p(f)=p(T)$.

证. 根据§1引理1，T 的极小多项式是

$$\tilde{f}(x)=x^n+\sum_{i=1}^{n}c_ix^{n-i}.$$

但 $f(x)$ 和 $\tilde{f}(x)$ 是互反的多项式，因此从定义 3 立刻推出 $p(f)=p(\tilde{f})$. 于是 $\tilde{f}(x)\mid x^{p(f)}-1$. 因 $\tilde{f}(T)=0$, 故 $T^{p(f)}=I$, 那么根据引理 5, $p(T)\mid p(f)$.

又从 $T^{p(T)}=I$ 推出 T 适合 $x^{p(T)}-1$. 但 $\tilde{f}(x)$ 是 T 的极小多项式，所以 $\tilde{f}(x)\mid x^{p(T)}-1$. 因此根据引理 3, $p(\tilde{f})\mid p(T)$. 于是 $p(f)\mid p(T)$.

因此 $p(f)=p(T)$.

定理 4 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中一个次数 $n\geqslant 1$ 而零次项等于 1 的多项式，那么以 $f(x)$ 为极小多项式的线性移位寄存器序列的周期就等于 $f(x)$ 的周期.

证. 设 $\mathbf{a}$ 是以 $f(x)$ 为极小多项式的线性移位寄存器序列. 写

$$f(x)=1+\sum_{i=1}^{n}c_ix^i,\ \ c_n\neq 0,$$

那么 $\mathbf{a}$ 适合

$$a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\quad k\geqslant n.$$

再设 T 是上述递归关系式所确定的变换矩阵，即 T 是 §1 第 (11) 式中的矩阵. 令

$$\mathbf{s}_k=(a_k,\ a_{k+1},\ a_{k+2},\ \cdots,\ a_{k+(n-1)}),\quad k\geqslant 0,$$

那么从 $T^{p(T)}=I$ 推出

$$\mathbf{s}_kT^{p(T)}=\mathbf{s}_k,\quad \text{对一切 } k\geqslant 0.$$

但 $\mathbf{s}_kT^{p(T)}=\mathbf{s}_{p(T)+k}$，所以

$$\mathbf{s}_{p(T)+k}=\mathbf{s}_k,\quad \text{对一切 } k\geqslant 0.$$

因此

$$a_{p(T)+k}=a_k,\quad \text{对一切 } k\geqslant 0.$$

那么根据引理 1 有 $p(\mathbf{a})\,|\,p(T)$. 根据引理 6, $p(T)=p(f)$，所以 $p(\mathbf{a})\,|\,p(f)$.

另一方面，$\mathbf{a}$ 适合线性递归关系式

$$a_k-a_{k-p(\mathbf{a})}=0,\quad k\geqslant p(\mathbf{a}),$$

其联接多项式是

$$1-x^{p(\mathbf{a})}.$$

因 $f(x)$ 是 $\mathbf{a}$ 的极小多项式，所以 $f(x)\,|\,x^{p(\mathbf{a})}-1$. 因此 $p(f)\,|\,p(\mathbf{a})$.

所以 $p(\mathbf{a})=p(f)$.

系理 1 设 $f(x)$ 是 $\mathbf{F}_q$ 上零次项等于 1 的 n 次不可约多项式，那么 $G(f)$ 中任一非零 q 元 n 级线性移位寄存器序列均以 $f(x)$ 为极小多项式，而且它们的周期都等于 $f(x)$ 的周期.

证. 设 $\mathbf{a}$ 是 $G(f)$ 中任一非零线性移位寄存器序列，那么根据定理 2, $\mathbf{a}$ 的极小多项式的次数 $\geqslant 1$，而且一定是 $f(x)$ 的因式. 但 $f(x)$ 不可约，所以 $\mathbf{a}$ 的极小多项式就是 $f(x)$，那么从定理 4 立刻推出 $p(\mathbf{a})=p(f)$.

系理 2 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个次数 $n\geqslant 1$ 的零次项等于 1 的多项式，那么 $G(f)$ 中从初始状态 $(0,\ 0,\ \cdots,\ 0,\ 1)$ 出

发的 q 元 n 级线性移位寄存器序列的周期等于 $f(x)$ 的周期.

证. 这是定理 3 和定理 4 的直接推论.

系理 3 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个次数 $n\geq 1$ 的零次项等于 1 的多项式，那么对于 $G(f)$ 中任一非零 q 元 n 级线性移位寄存器序列 $\mathbf{a}$, 都有 $p(\mathbf{a})\mid p(f)$.

证. 设 $\mathbf{a}$ 的极小多项式是 $h(x)$. 根据定理 2, $\partial^0 h(x)\geq 1$ 而 $h(x)\mid f(x)$. 根据定理 4, $p(\mathbf{a})=p(h)$. 但 $f(x)\mid x^{p(f)}-1$, 所以 $h(x)\mid x^{p(f)}-1$. 于是 $p(h)\mid p(f)$. 因此 $p(\mathbf{a})\mid p(f)$.

§3 $G(f)$ 中的平移等价类

在这一节里，我们总假定 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个零次项等于 1 的 n 次多项式，而 $n\geq 1$. 我们写

$$f(x)=1+c_1x+c_2x^2+\cdots+c_nx^n,\ c_n\neq 0,\ c_i\in\mathbf{F}_q. \tag{1}$$

设 $\mathbf{a}$ 是一个 q 元序列，写

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),\ \ a_i\in\mathbf{F}_q, \tag{2}$$

那么 $\mathbf{a}\in G(f)$, 当且仅当

$$c_0a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\ k\geq n. \tag{3}$$

我们先引进 q 元周期序列的左移变换.

定义 1 设 $\mathbf{a}$ 是个 q 元周期序列，将 $\mathbf{a}$ 写作(2). 定义作用在 $\mathbf{a}$ 上的*左移变换* L:

$$L(\mathbf{a})=(a_1,\ a_2,\ a_3,\ \cdots).$$

并定义

$$L^0(\mathbf{a})=\mathbf{a}$$

$$L^t(\mathbf{a})=(\underbrace{L(L\cdots(L}_{t\text{个}}(\mathbf{a}))\cdots)),$$

这里 t 是个正整数.

定义 2 设 $\mathbf{a}$ 和 $\mathbf{b}$ 都是 q 元周期序列，如果有非负整数 t 存在使 $\mathbf{b}=L^t(\mathbf{a})$, 那么就说 $\mathbf{a}$ 与 $\mathbf{b}$ *平移等价*. 平移不等

价的周期序列叫平移相异.

引理1 设 $\mathbf{a}$ 和 $\mathbf{b}$ 都是 q 元周期序列，如果 $\mathbf{a}$ 与 $\mathbf{b}$ 平移等价，则 $\mathbf{b}$ 与 $\mathbf{a}$ 平移等价.

证. 设 $\mathbf{a}$ 的周期是 $p(\mathbf{a})$. 因 $\mathbf{a}$ 与 $\mathbf{b}$ 平移等价，有非负整数 t 存在使 $\mathbf{b}=L^t(\mathbf{a})$，即

$$b_k=a_{t+k},\quad k\geqslant 0.$$

根据带余除法，可以写

$$t=qp(\mathbf{a})+r,\quad 0\leqslant r<p(\mathbf{a}),$$

那么

$$\begin{aligned}a_k&=a_{(q+1)p(\mathbf{a})+k}=a_{t+p(\mathbf{a})-r+k}\\&=b_{p(\mathbf{a})-r+k},\quad k\geqslant 0.\end{aligned}$$

因此 $\mathbf{a}=L^{p(\mathbf{a})-r}(\mathbf{b})$，即 $\mathbf{b}$ 与 $\mathbf{a}$ 平移等价.

引理2 设 $\mathbf{a}$ 和 $\mathbf{b}$ 都是 q 元周期序列. 如果 $\mathbf{a}$ 和 $\mathbf{b}$ 平移等价，那么 $p(\mathbf{a})=p(\mathbf{b})$. 更进一步，

$$\mathbf{a},\ L(\mathbf{a}),\ L^2(\mathbf{a}),\ \cdots,\ L^{p(\mathbf{a})-1}(\mathbf{a}) \tag{4}$$

是所有与 $\mathbf{a}$ 平移等价的两两相异的 q 元周期序列，而

$$L^{p(\mathbf{a})}(\mathbf{a})=\mathbf{a}.$$

证. 设 $\mathbf{b}=L^t(\mathbf{a})$，即

$$b_k=a_{t+k},\quad k\geqslant 0,$$

那么

$$b_{p(\mathbf{a})+k}=a_{t+p(\mathbf{a})+k}=a_{t+k}=b_k,\quad k\geqslant 0.$$

根据 §2 引理 1，$p(\mathbf{b})\,|\,p(\mathbf{a})$. 同理可证 $p(\mathbf{a})\,|\,p(\mathbf{b})$. 因此 $p(\mathbf{a})=p(\mathbf{b})$.

再设

$$L^i(\mathbf{a})=L^j(\mathbf{a}),\ 0\leqslant i\leqslant j<p(\mathbf{a}),$$

那么

$$a_{i+k}=a_{j+k},\quad k\geqslant 0.$$

于是

$$a_{(j-i)+k}=a_{j+(k-i)}=a_{i+(k-i)}=a_k,\ k\geqslant i,$$

这就是说，如果 $i\neq j$，$L^i(\mathbf{a})$ 的周期是 $j-i$ 的因子，因此 $\mathbf{a}$ 的周期也是 $j-i$ 的因子. 但 $j-i<p(\mathbf{a})$. 因此一定有 $i=j$. 所以 (4) 中 $p(\mathbf{a})$ 个序列两两相异.

最后，因 $\mathbf{a}$ 的周期是 $p(\mathbf{a})$，显然有

$$L^{p(\mathbf{a})}(\mathbf{a})=\mathbf{a}.$$

定义 3 一组 q 元周期序列叫做一个平移等价类，如果其中任意两个序列都平移等价，而与这个组里任意一个序列平移等价的序列都在这个组里.

那么由引理 1 和引理 2 立刻推出

定理 1 设 $\mathbf{a}$ 是个 q 元周期序列，周期等于 $p(\mathbf{a})$. 那么含 $\mathbf{a}$ 的平移等价类就是

$$C=\{\mathbf{a},\ L(\mathbf{a}),\ L^2(\mathbf{a}),\ \cdots,\ L^{p(\mathbf{a})-1}(\mathbf{a})\}. \tag{5}$$

更进一步，两个 q 元周期序列的平移等价类或者完全一致或者没有公共元素.

证. 显然(5)中任意两个周期序列都平移等价. 再设 q 元周期序列 $\mathbf{b}$ 与 $L^t(\mathbf{a})$ 平移等价，可以假定

$$\mathbf{b}=L^s(L^t(\mathbf{a}))$$

那么
$$\mathbf{b}=\begin{cases}L^{s+t}(\mathbf{a}), & \text{如果 } s+t<p(\mathbf{a}),\\ L^{s+t-p(\mathbf{a})}(\mathbf{a}), & \text{如果 } s+t\geqslant p(\mathbf{a}).\end{cases}$$

因此 $\mathbf{b}\in C$.

更进一步，设有两个 q 元周期序列的平移等价类 C_1 和 C_2 有一个序列公共. 设 $\mathbf{a}\in C_1\cap C_2$. 假定 $\mathbf{a}$ 的周期是 $p(\mathbf{a})$. 那么 C_1 和 C_2 就都是 C. 因此 $C_1=C_2$.

系理 1 q 元周期序列的一个平移等价类中的元素个数就等于它里面任意一个序列的周期.

系理 2 所有 q 元周期序列的集合分到了一些两两没有公共元素的平移等价类里.

特别还有

系理 3 $G(f)$ 中的 q 元周期序列分到了一些两两没有公共元素的平移等价类里.

证. 这是因为，如果 $\mathbf{a}\in G(f)$，那么 $L(\mathbf{a})\in G(f)$，于是含 $\mathbf{a}$ 的 q 元周期序列的平移等价类中的序列都属于 $G(f)$.

在§1例1里，我们说过，§1图1的二元4级线性移位寄存器总共产生四个完全不同的线性移位寄存器序列．那里说的“完全不同的”实际上就是上面定义的“平移不等价的”．因此我们可以说，§1图1的二元4级线性移位寄存器产生的线性移位寄存器序列分属四个平移等价类．同样，§1例2中的线性移位寄存器产生的线性移位寄存器序列分属两个平移等价类；而§1例3中的线性移位寄存器产生的线性移位寄存器序列分属四个平移等价类．§1例1和例3的两个线性移位寄存器所产生的线性移位寄存器序列虽然都分成四个平移等价类，但例1的四个类中的序列的个数分别是1，5，5，5，而例3中四个类中序列的个数却分别是1，6，6，3．我们知道例1和例3的线性移位寄存器的联接多项式不一样：一个是$1+x+x^2+x^3+x^4$，而另一个是$1+x^2+x^4$．下面我们要证明，一个非退化的q元n级线性移位寄存器所产生的线性移位寄存器序列一共分成多少平移等价类，以及每一类里含多少个序列，由它的联接多项式$f(x)$所完全确定，即$G(f)$一共分成多少类，以及每一类里有多少个元素，由$f(x)$所完全确定．

我们先证明

定理2 设$f(x)$是$\mathbf{F}_q[x]$中的一个零次项等于1的n次多项式，而$n\geqslant 1$．并假定

$$f(x)=f_1(x)f_2(x)\cdots f_r(x), \tag{6}$$

其中$f_i(x)\,(1\leqslant i\leqslant r)$是零次项等于1的$n_i$次多项式，$n_i\geqslant 1$，而且$f_1(x)$，$f_2(x)$，…，$f_r(x)$两两互素，即

$$(f_i(x),\ f_j(x))=1,\ \text{如果}\ i\neq j, \tag{7}$$

那么$G(f)$作为$\mathbf{F}_q$上的n维向量空间，分解成子空间$G(f_1)$，$G(f_2)$，…，$G(f_r)$的直和：

$$G(f)=G(f_1)\dot{+}G(f_2)\dot{+}\cdots\dot{+}G(f_r).$$

证. 因 $f_i(x)|f(x)$ $(1\leqslant i\leqslant r)$, 所以根据 §2 定理 2 $G(f_i)\subset G(f)$, 又因 $G(f)$ 和 $G(f_i)$ 中的加法都是按分量相加, 即按 §1 中 (12) 式所定义, 而用 $\mathbf{F}_q$ 的元素去乘 $G(f)$ 和 $G(f_i)$ 中元素的乘法又都是按 §1 (13) 式所定义, 所以 $G(f_i)$ $(1\leqslant i\leqslant r)$ 都是 $G(f)$ 的子空间.

因 $\partial^0 f_i(x)=n_i$, 所以 $G(f_i)$ 是 $\mathbf{F}_q$ 上的 n_i 维子空间. 设

$$\mathbf{a}_{i1},\ \mathbf{a}_{i2},\ \cdots,\ \mathbf{a}_{in_i}$$

是 $G(f_i)$ 的一组基, $1\leqslant i\leqslant r$. 我们来证明

$$\mathbf{a}_{11},\ \mathbf{a}_{12},\ \cdots,\ \mathbf{a}_{1n_1},\ \mathbf{a}_{21},\ \mathbf{a}_{22},\ \cdots,\ \mathbf{a}_{2n_2},\ \cdots,\ \mathbf{a}_{r1},\ \mathbf{a}_{r2},\ \cdots,\ \mathbf{a}_{rn_r} \tag{8}$$

一定线性无关. 设有线性关系

$$\sum_{i=1}^{r}\sum_{j=1}^{n_i} c_{ij}\mathbf{a}_{ij}=\mathbf{0},\quad c_{ij}\in\mathbf{F}_2.$$

其中 $\mathbf{0}=(0,\ 0,\ 0,\ \cdots)$ 是零序列. 令

$$\mathbf{a}_i=\sum_{j=1}^{n_i} c_{ij}\mathbf{a}_{ij},$$

那么 $$\mathbf{a}_i\in G(f_i)\ (1\leqslant i\leqslant r),$$

而 $$\mathbf{a}_1+\mathbf{a}_2+\cdots+\mathbf{a}_r=\mathbf{0}. \tag{9}$$

如果 $\mathbf{a}_1\neq 0$, 那么

$$\mathbf{a}_1=-(\mathbf{a}_2+\cdots+\mathbf{a}_r).$$

于是 $$\mathbf{a}_1\in G(f_2\cdot f_3\cdot\cdots\cdot f_r).$$

设 $\mathbf{a}_1$ 的极小多项式是 $m(x)$, 那么根据 §2 定理 2 有

$$m(x)|f_1(x),\ m(x)|f_2(x)f_3(x)\cdots f_r(x).$$

但由(7)式推出

$$(f_1(x),\ f_2(x)f_3(x)\cdots f_r(x))=1.$$

因此 $m(x)=1$, 所以

$$\mathbf{a}_1=\mathbf{0}=(0,\ 0,\ 0,\ \cdots).$$

同理可证 $$\mathbf{a}_2=\mathbf{a}_3=\cdots=\mathbf{a}_r=\mathbf{0}.$$

因此 $$\sum_{j=1}^{n_i} c_{ij}\mathbf{a}_{ij}=\mathbf{0},\ 1\leqslant i\leqslant r.$$

因 $\mathbf{a}_{i1}, \mathbf{a}_{i2}, \cdots, \mathbf{a}_{in_i}$ 是 $G(f_i)$ 的一组基，所以

$$c_{ij}=0.\ i=1,\ 2,\ \cdots,\ r;\ j=1,\ 2,\ \cdots,\ n_r.$$

这证明了(8)线性无关。但由(6)式推出

$$n=n_1+n_2+\cdots+n_r,$$

而 $\dim G(f)=n$，所以(8)是 $G(f)$ 的一组基.

设 $\mathbf{b}\in G(f)$，那么 $\mathbf{b}$ 可以表成(8)中序列的线性组合

$$\mathbf{b}=\sum_{i=1}^{r}\sum_{j=1}^{n_i} b_{ij}\mathbf{a}_{ij},\quad b_{ij}\in \mathbf{F}_q.$$

令 $$\mathbf{b}_i=\sum_{j=1}^{n_i} b_{ij}\mathbf{a}_{ij},\ 1\leqslant i\leqslant r,$$

那么 $\mathbf{b}_i\in G(f_i)$ 而

$$\mathbf{b}=\mathbf{b}_1+\mathbf{b}_2+\cdots+\mathbf{b}_r. \tag{10}$$

这证明了 $G(f)$ 中的一个元素 $\mathbf{b}$ 可以表成 $G(f_1)$ 中一个元素 $\mathbf{b}_1$, $G(f_2)$ 中一个元素 $\mathbf{b}_2$, $\cdots$, $G(f_i)$ 中一个元素 $\mathbf{b}_r$ 的和. 如果 $\mathbf{b}$ 还有另一种表法

$$\mathbf{b}=\mathbf{c}_1+\mathbf{c}_2+\cdots+\mathbf{c}_r,\ \mathbf{c}_i\in G(f_i), \tag{11}$$

那么将(10), (11) 两式相减，得到

$$(\mathbf{b}_1-\mathbf{c}_1)+(\mathbf{b}_2-\mathbf{c}_2)+\cdots+(\mathbf{b}_r-\mathbf{c}_r)=\mathbf{0},$$
$$\mathbf{b}_i-\mathbf{c}_i\in G(f_i),$$

可以重复前面从(9)式推出 $\mathbf{a}_1=\mathbf{a}_2=\cdots=\mathbf{a}_r=\mathbf{0}$ 的证明

推出 $$\mathbf{b}_i-\mathbf{c}_i=\mathbf{0},\ i=1,\ 2,\ \cdots,\ r.$$

于是 $$\mathbf{b}_i=\mathbf{c}_i,\ i=1,\ 2,\ \cdots,\ r.$$

这证明了表法的唯一性. 因此

$$G(f)=G(f_1)\dot{+}G(f_2)\dot{+}\cdots\dot{+}G(f_r).$$

再证明下面这个引理.

引理 3 设 $f_1(x)$, $f_2(x)$ 都是 $\mathbf{F}_q[x]$ 中零次项等于 1 的次数 $\geqslant 1$ 的多项式，并假定 $(f_1(x), f_2(x))=1$，再设 $\mathbf{a}\in$

$G(f_1)$, $\mathbf{b}\in G(f_2)$, 那么

$$p(\mathbf{a}+\mathbf{b})=[p(\mathbf{a}),\ p(\mathbf{b})],$$

其中 $p(\mathbf{a})$, $p(\mathbf{b})$, $p(\mathbf{a}+\mathbf{b})$ 分别表 $\mathbf{a}$, $\mathbf{b}$, $\mathbf{a}+\mathbf{b}$ 的周期.

证. 设 $l=[p(\mathbf{a}),p(\mathbf{b})]$, $l'=p(\mathbf{a}+\mathbf{b})$. 再设

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$
$$\mathbf{b}=(b_0,\ b_1,\ b_2,\ \cdots).$$

考察有序对的序列

$$(a_0,\ b_0),\ (a_1,\ b_1),\ (a_2,\ b_2),\ \cdots$$

设它的周期是 s, 那么显然 $s|l$. 但显然 $l'|s$. 因此 $l'|l$.

因 $p(\mathbf{a}+\mathbf{b})=l'$, 所以

$$a_{l'+k}+b_{l'+k}=a_k+b_k,\quad k\geqslant 0.$$

于是 $$a_{l'+k}-a_k+b_{l'+k}-b_k=0,\quad k\geqslant 0.$$

这就是说 $$(L^{l'}(\mathbf{a})-\mathbf{a})+(L^{l'}(\mathbf{b})-\mathbf{b})=\mathbf{0}.$$

但 $$L^{l'}(\mathbf{a})-\mathbf{a}\in G(f_1),\ L^{l'}(\mathbf{b})-\mathbf{b}\in G(f_2),$$

而根据定理 2, $G(f)$ 分解成 $G(f_1)$ 和 $G(f_2)$ 的直和, 特别 $\mathbf{0}$ 只有一种方法表成 $G(f_1)$ 中的一个元素与 $G(f_2)$ 中的一个元素的和:

$$\mathbf{0}=\mathbf{0}+\mathbf{0},$$

因此一定有 $$L^{l'}(\mathbf{a})-\mathbf{a}=\mathbf{0},\ L^{l'}(\mathbf{b})-\mathbf{b}=\mathbf{0}.$$

于是 $$L^{l'}(\mathbf{a})=\mathbf{a},\ L^{l'}(\mathbf{b})=\mathbf{b}.$$

由此推出 $p(\mathbf{a})|l'$, $p(\mathbf{b})|l'$. 因 $l=[p(\mathbf{a}),\ p(\mathbf{b})]$, 所以 $l|l'$.

从 $l'|l$ 和 $l|l'$ 推出 $l=l'$. 即 $p(\mathbf{a}+\mathbf{b})=[p(\mathbf{a}),\ p(\mathbf{b})]$.

显然引理 3 可推广到 r 个两两互素的多项式的情形.

引理 4 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个零次项等于 1 的 n 次多项式, 而 $n\geqslant 1$. 并假定

$$f(x)=f_1(x)f_2(x)\cdots f_r(x),$$

其中 $f_i(x)\ (1\leqslant i\leqslant r)$ 是零次项等于 1 的 n_i 次多项式, $n_i\geqslant 1$,

而 $f_1(x)$, $f_2(x)$, …, $f_r(x)$ 两两互素. 再设 $\mathbf{a}_i \in G(f_i)$, $1 \leqslant i \leqslant r$, 那么

$$p(\mathbf{a}_1+\mathbf{a}_2+\cdots+\mathbf{a}_r)=[p(\mathbf{a}_1),\ p(\mathbf{a}_2),\ \cdots,\ p(\mathbf{a}_r)]$$

由于这个引理的证明和引理 3 的证明完全一样, 我们就不重复了.

从定理 2 和引理 4 可以推出

定理 3 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个零次项等于 1 的 n 次多项式, 而 $n \geqslant 1$, 并假定

$$f(x)=f_1(x)f_2(x)\cdots f_r(x),$$

其中 $f_i(x)$ 是零次项等于 1 的 n_i 次多项式, $n_i \geqslant 1$, 而 $f_1(x)$, $f_2(x)$, …, $f_r(x)$ 两两互素, 再假定 $G(f_i)$ $(1 \leqslant i \leqslant r)$ 分成了 m_i 个平移等价类

$$C_{i1},\ C_{i2},\ \cdots,\ C_{im_i} (i=1,\ 2,\ \cdots,\ r)$$

而 C_{ij} 中序列的周期分别是 p_{ij} $(i=1,\ 2,\ \cdots,\ r;\ j=1,\ 2,\ \cdots,\ m_i)$. 令

$$C_{k_1k_2\cdots k_r}=\{\mathbf{a}_{1k_1}+\mathbf{a}_{2k_2}+\cdots+\mathbf{a}_{rk_r} \mid \mathbf{a}_{ik_i} \in C_{ik_i},\ i=1,\ 2,\ \cdots,\ r\},$$
$$k_i=1,\ 2,\ \cdots,\ m_i;\ i=1,\ 2,\ \cdots,\ r,$$

那么 $C_{k_1k_2\cdots k_r}$ 中序列的周期是

$$[p_{1k_1},\ p_{2k_2},\ \cdots,\ p_{rk_r}]$$

而 $C_{k_1k_2\cdots k_r}$ 分成

$$p_{1k_1}p_{2k_2}\cdots p_{rk_r}/[p_{1k_1},\ p_{2k_2},\ \cdots,\ p_{rk_r}]$$

个平移等价类. 这样 $G(f)$ 就分成

$$\sum_{k_1=1}^{m_1}\sum_{k_2=1}^{m_2}\cdots\sum_{k_r=1}^{m_r} p_{1k_1}p_{2k_2}\cdots p_{rk_r}/[p_{1k_1},\ p_{2k_2},\ \cdots,\ p_{rk_r}]$$

个平移等价类.

证. 首先注意. C_{ij} 中序列的周期是 p_{ij}, 那么 C_{ij} 中序列的个数 $|C_{ij}|$ 也是 p_{ij}.

设 $$\mathbf{a}_{k_1k_2\cdots k_r} \in C_{k_1k_2\cdots k_r}.$$

那么 $\quad \mathbf{a}_{k_1k_2\cdots k_r}=\mathbf{a}_{1k_1}+\mathbf{a}_{2k_2}+\cdots+\mathbf{a}_{rk_r},\ \mathbf{a}_{ik_i}\in C_{ik_i},$

于是 $\quad L(\mathbf{a}_{k_1k_2\cdots k_r})=L(\mathbf{a}_{1k_1})+L(\mathbf{a}_{2k_2})+\cdots+(\mathbf{a}_{rk_r}).$

但 C_{ik_i} 是$G(f_i)$ 的一个平移等价类，所以

$$L(\mathbf{a}_{ik_i})\in C_{ik_i},\ i=1,\ 2,\ \cdots,\ r;\ k_i=1,\ 2,\ \cdots,\ m_i.$$

因此 $\quad L(\mathbf{a}_{k_1k_2\cdots k_r})\in C_{k_1k_2\cdots k_r}.$

这证明了 $C_{k_1k_2\cdots k_r}$ 由一些平移等价类组成. 根据引理4, $C_{k_1k_2\cdots k_r}$ 中序列的周期都等于 $[p_{1k_1},\ p_{2k_2},\ \cdots,\ p_{rk_r}]$, 所以 $C_{k_1k_2\cdots k_r}$ 中的每一个平移等价类都含 $[p_{1k_1},\ p_{2k_2},\ \cdots,\ p_{rk_r}]$ 个序列. 另一方面，根据定理 2

$$G(f)=G(f_1)\dot{+}G(f_2)\dot{+}\cdots\dot{+}G(f_r),$$

所以 $C_{k_1k_2\cdots k_r}$ 中序列的个数

$$|C_{k_1k_2\cdots k_r}|=|C_{1k_1}|\,|C_{2k_2}|\cdots|C_{rk_r}|=p_{1k_1}p_{2k_2}\cdots p_{rk_r},$$

因此 $C_{k_1k_2\cdots k_r}$ 分成了

$$p_{1k_1}p_{2k_2}\cdots p_{rk_r}/[p_{1k_1},\ p_{2k_2},\ \cdots,\ p_{rk_r}]$$

个平移等价类.

又因 $\quad G(f_i)=C_{i1}\cup C_{i2}\cup\cdots\cup C_{im_i},\ i=1,\ 2,\ \cdots,\ r,$

所以根据定理 2 就有

$$G(f)=\bigcup_{\substack{1\leq k_i\leq m_i\\ 1\leq i\leq r}} C_{k_1k_2\cdots k_r}.$$

由上式就可以推出本定理的最后一个断言.

根据唯一因式分解定理知，$\mathbf{F}_q[x]$ 中每一个次数 $n\geqslant 1$ 的零次项等于1 的多项式 $f(x)$ 都可以表成

$$f(x)=p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_r(x)^{e_r},$$

其中 $p_1(x),\ p_2(x),\ \cdots,\ p_r(x)$ 是 $\mathbf{F}_q[x]$ 中的 r 个两两不同的零次项等于1 的不可约多项式，而 $e_1,\ e_2,\ \cdots,\ e_r$ 都是正整数，那么从定理3 就可得出结论，只要对 $\mathbf{F}_q$ 上零次项等于1 的不可约多项式 $f(x)$ 的幂 $f(x)^e$, 研究 $G(f(x)^e)$ 分成多少平移等价类，而每个类里含多少个序列即可. 我们先证明

引理5 设$f(x)$是$\mathbf{F}_q$上的一个零次项等于1的不可约多项式，q是一个素数p的幂，而e是一个正整数．令

$$m=\min\{i\,|\,i\in\mathbf{J}\text{ 而 }p^i\geqslant e\},$$

即m是一个正整数使$p^m\geqslant e>2^{m-1}$，那么

$$p(f^e)=p^m p(f).$$

证．根据多项式的周期的定义，我们有

$$f(x)\,|\,x^{p(f)}-1.$$

因此
$$f(x)^{p^m}\,|\,(x^{p(f)}-1)^{p^m}.$$

我们有
$$(x^{p(f)}-1)^{p^m}=x^{p^m p(f)}-1.$$

又因$p^m\geqslant e$，所以

$$f(x)^e\,|\,f(x)^{p^m},$$

因此
$$f(x)^e\,|\,x^{p^m p(f)}-1,$$

于是
$$p(f^e)\,|\,p^m p(f).$$

另一方面，设$p(f^e)=p^j\cdot t$，而$p\nmid t$，那么

$$f(x)^e\,|\,x^{p^j t}-1.$$

因
$$x^{p^j t}-1=(x^t-1)^{p^j},$$

所以

$$f(x)^e\,|\,(x^t-1)^{p^j}. \tag{12}$$

因
$$p\nmid t,\ (x^t-1)'=tx^{t-1}\neq 0,\ \text{所以}$$
$$(x^t-1,\ (x^t-1)')=1,$$

那么根据第一章§2定理3，x^t-1就没有重因式．又因$f(x)$是不可约多项式，所以从(12)式根据唯一因式分解定理推出

$$f(x)\,|\,x^t-1,\ e\leqslant p^j.$$

因此$p(f)\,|\,t$，而$m\leqslant j$．所以

$$p^m p(f)\,|\,p(f^e).$$

因此
$$p(f^e)=p^m p(f).$$

现在我们证明

定理4 设$f(x)$是$\mathbf{F}_q$上的一个零次项等于1的n次不

可约多项式，q 是一个素数 p 的幂而 e 是一个正整数．再设

$$m=\min\{i \mid i\in \mathbf{J} \text{ 而 } p^i\geqslant e\},$$

那么只有 1, $p(f)$, $p^j p(f)$ $(j=1, 2, \cdots, m-1)$, $p^m p(f)$ 这些数可以作为 $G(f^e)$ 中序列的周期；而 $G(f^e)$ 中以这些数为周期的序列的个数分别是 1, q^n-1, $q^{np^i}-q^{np^{i-1}}$ $(i=1, 2, \cdots, m-1)$, $q^{ne}-q^{np^{m-1}}$；因此 $G(f)$ 中以这些数为周期的平移等价类的个数分别是 1, $(q^n-1)/p(f)$, $(q^{np^j}-q^{np^{i-1}})/p^i p(f)$ $(i=1, 2, \cdots, m-1)$, $(q^{ne}-q^{np^{m-1}})/p^m p(f)$.

证．因 $f(x)$ 是不可约多项式，$G(f^e)$ 中任一序列的极小多项式一定是 $f(x)$ 的一个幂．考察升链

$$G(f^0)\subset G(f^1)\subset G(f^2)\subset\cdots\subset G(f^e).$$

显然 $G(f^0)=\{\mathbf{0}\}$．因此

$$|G(f^0)|=1,$$

而 $G(f^0)$ 中唯一的序列 $\mathbf{0}$ 的周期是 1.

其次，对 $i=0, 1, 2, \cdots, e-1$, $G(f^{i+1})\backslash G(f^i)$ 中序列以 $f(x)^{i+1}$ 为极小多项式．因此根据 §2 定理 4, $G(f^{i+1})\backslash G(f^i)$ 中序列的周期即是 $p(f^{i+1})$．根据引理 5，我们有

$$p(f^{p^{i-1}+1})=p(f^{p^{i-1}+2})=\cdots=p(f^{p^i})=p^i p(f)$$
$$(i=1, 2, \cdots, m-1),$$
$$p(f^{p^{m-1}+1})=p(f^{p^{m-1}+2})=\cdots=p(f^e)=p^m p(f),$$

因此 $G(f^e)$ 中只有 $G(f)\backslash G(f^0)$ 中序列的周期是 $p(f)$，而

$$|G(f)\backslash G(f^0)|=q^n-1.$$

$G(f^e)$ 中只有

$$\bigcup_{1<j<(p-1)p^{i-1}}(G(f^{p^{i-1}+j})\backslash G(f^{p^{i-1}+(j-1)}))=G(f^{p^i})\backslash G(f^{p^{i-1}})$$
$$(i=1, 2, \cdots, m-1)$$

中序列的周期是 $p^i p(f)$，而

$$|G(f^{p^i})\backslash G(f^{p^{i-1}})|=q^{np^i}-q^{np^{i-1}}.$$

同理，$G(f^e)$ 中只有

$$\bigcup_{1\leqslant j\leqslant e-p^{m-1}}\left(G(f^{p^{m-1}+j})\backslash G(f^{p^{m-1}+(j-1)})\right)=G(f^e)\backslash G(f^{p^{m-1}})$$

中序列的周期是 $p^m p(f)$，而

$$|G(f^e)\backslash G(f^{p^{m-1}})|=q^{ne}-q^{np^{m-1}}.$$

这样定理 4 就完全证明了.

从定理 4 我们知道，计算不可约多项式的周期很重要，这个问题将在第五章中讨论.

我们看几个例子.

例 1 考察 $\mathbf{F}_2$ 上的多项式 $f(x)=x^3+x+1$.

先计算 $f(x)$ 的周期 $p(f)$. 因 $f(0)\neq 0$, $f(1)\neq 0$, 所以 $f(x)$ 没有一次因式. 因 $\partial^0 f(x)=3$, 所以 $f(x)$ 不可约. 根据第一章 §5 引理 2, $f(x)\mid x^{2^3-1}-1=x^7-1$. 根据 §2 引理 3, $p(f)\mid 7$. 因 7 是素数，所以 $p(f)=7$.

$|G(f)|=2^3=8$. $G(f)$ 中一共有 7 个非零序列；根据 §2定理 4 的系理 1，它们的周期都等于 $p(f)$，即都等于 7. 即它们都是m序列.

例 2 考察 $\mathbf{F}_2$ 上的多项式 $f(x)^3=(x^3+x+1)^3$.

根据定理 4, 只有 1, $p(f)=7$, $2p(f)=14$, $2^2p(f)=28$ 这 4 个数可以作为 $G(f^3)$ 中序列的周期, $G(f^3)$ 中以这 4 个数为周期的序列的个数分别是 1, $2^3-1=7$, $2^{3\cdot 2}-2^3=56$, $2^{3\cdot 3}-2^{3\cdot 2}=448$, 而 $G(f^3)$ 中以这些数为周期的平移等价类的个数分别是 1, 1, 4, 16.

例 3 考察 $\mathbf{F}_2$ 上的多项式 $f(x)=(x^2+x+1)^3(x^4+x+1)$.

令 $f_1(x)=x^2+x+1$, $f_2(x)=x^4+x+1$.

容易证明 $f_1(x)$ 不可约. 那么 $f_1(x)\mid x^{2^2-1}-1=x^3-1$. 因 3 是素数，所以 $p(f_1)=3$.

根据定理4, $G(f_1^3)$中的序列以1, $p(f)=3$, $2p(f)=6$或$2^2p(f)=12$为周期; 有1个平移等价类C_{11}以1为周期, $|C_{11}|=1$; 有1个平移等价类C_{12}以3为周期, $|C_{12}|=3$; 有2个平移等价类C_{13}, C_{14}以6为周期, $|C_{13}|=|C_{14}|=6$; 有4个平移等价类C_{15}, C_{16}, C_{17}, C_{18}以12为周期.

根据§1例2, $G(f_2)$中有一个序列以15为周期, 但$15=2^4-1$, 因此这是个m序列. 这样$G(f_2)$就分成两个平移等价类C_{21}和C_{22}, 而$|C_{21}|=1$, $|C_{22}|=15$.

再根据定理3, C_{21}中的零序列与$G(f_1^3)$中任一平移等价类中的序列相加就得到$G(f)$的一个平移等价类, 这样一共得到8个类: 1个只含1个序列的类, 即含**0**的类, 1个含3个序列的类, 2个各含6个序列的类, 4个各含12个序列的类. C_{22}中的序列与C_{11}中序列相加得到1个含15个序列的类; C_{22}中的序列与C_{12}中序列相加得到3个含15个序列的类; C_{22}中的序列与C_{13}或C_{14}中的序列相加得到6个各含30个序列的类; C_{22}中的序列与C_{15}或C_{16}或C_{17}或C_{18}中的序列相加得到12个各含60个序列的类.

因此$G(f)$总共分成30个平移等价类, 它们之中有1个类含1个序列, 1个类含3个序列, 2个类各含6个序列, 4个类各含12个序列, 4个类各含15个序列, 6个类各含30个序列, 12个类各含60个序列.

现在我们来引进线性移位寄存器的状态图, 它有助于我们进一步理解线性移位寄存器序列, 特别还可以给出定理3和定理4的一个图论解释.

设有一q元n级线性移位寄存器, 它的联接多项式是零次项等于1的多项式

$$f(x)=1+c_1x+c_2x^2+\cdots+c_nx^n,\ c_i\in\mathbf{F}_q,$$

它的每一个寄存器个可以独立地取$\mathbf{F}_q$中的q个元素之一作

为状态. 因此这个 n 级线性移位寄存器一共有 q^n 个可能的状态. 我们说这个移位寄存器居于状态 $(a_1, a_2, \cdots, a_n)$, $a_i \in \mathbf{F}_q$, 意思是说, 它的第 i 个寄存器的状态是 $a_{n-i+1}(i=1, 2, \cdots, n)$. 我们总把状态 $(a_1, a_2, \cdots, a_n)$ 看作 $V_n(\mathbf{F}_q)$ 中的元素, 而

$$V_n(\mathbf{F}_q) = \{(a_1, a_2, \cdots, a_n) \mid a_1, a_2, \cdots, a_n \in \mathbf{F}_q\},$$

这样 $V_n(\mathbf{F}_q)$ 就是这个移位寄存器的状态集. 现在设这个移位寄存器居于状态 $(a_1, a_2, \cdots, a_n)$, 那么加上一个移位脉冲之后, 这个移位寄存器的状态就成为 $(a_2, a_3, \cdots, a_n, a_{n+1})$, 而

$$a_{n+1} = -(c_1 a_n + c_2 a_{n-1} + \cdots + c_n a_1).$$

因此这个移位寄存器就确定了一个状态转移变换 T_f:

$$\begin{aligned} T_f\colon &(a_1, a_2, \cdots, a_n) \\ &\to (a_2, \cdots, a_n, -(c_1 a_n + c_2 a_{n-1} + \cdots + c_n a_1)). \end{aligned}$$

我们在前面已经知道, 状态转移变换可以将原状态 $(a_1, a_2, \cdots, a_n)$ 右乘以状态转移矩阵

$$T = \begin{pmatrix} 0 & & & & -c_n \\ 1 & 0 & & & -c_{n-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -c_2 \\ & & & 1 & -c_1 \end{pmatrix}$$

来实现, 即

$$\begin{aligned} &(a_2, \cdots, a_n, -(c_1 a_n + c_2 a_{n-1} + \cdots + c_n a_1)) \\ &= (a_1, a_2, \cdots, a_n) T. \end{aligned}$$

我们可以用平面上 q^n 个点来代表一个 q 元 n 级移位寄存器的 q^n 个状态, 在每个点的附近标上它所代表的状态. 我们把这每一个点叫做一个顶点. 如果一个状态 $(a_1, a_2, \cdots, a_n)$ 经过这个移位寄存器的状态转移变换 T_f 变到了另一个状态 $(a_2, \cdots, a_n, a_{n+1})$, 其中 $a_{n+1} = -(c_1 a_n + c_2 a_{n-1} + \cdots + c_n a_1)$, 我们就画一条连接代表状态 $(a_1, a_2, \cdots, a_n)$ 的顶点和代表状态 $(a_2, \cdots, a_n, a_{n+1})$ 的顶点的带箭头的线段 (直线段或曲线

段)，箭头指向从 $(a_1, a_2, \cdots, a_n)$ 到 $(a_2, \cdots, a_n, a_{n+1})$. 我们把这样一个带箭头的线段叫做从 $(a_1, a_2, \cdots, a_n)$ 到 $(a_2, \cdots, a_n, a_{n+1})$ 的弧，简称弧. $(a_1, a_2, \cdots, a_n)$ 叫做这条弧的起点，$(a_2, a_3, \cdots, a_n, a_{n+1})$ 叫做这条弧的终点. 这样我们就得到一个有向图，它有 q^n 个顶点，q^n 条弧，每一个顶点有一条且仅一条弧以它为起点. 这个有向图就叫这个 q 元 n 级线性移位寄存器的状态转移图，简称状态图，记作 G_f. 设 G_f 中有一条弧以 $(a_1, a_2, \cdots, a_n)$ 为起点而以 $(a_2, a_3, \cdots, a_n, a_{n+1})$ 为终点，我们就说 $(a_1, a_2, \cdots, a_n)$ 是 $(a_2, a_3, \cdots, a_n, a_{n+1})$ 的先导，而 $(a_2, a_3, \cdots, a_n, a_{n+1})$ 是 $(a_1, a_2, \cdots, a_n)$ 的后继. 显然 G_f 的每个顶点都有唯一的一个后继.

例如，§1 例 1, 例 2 和例 3 中的二元 4 级线性移位寄存

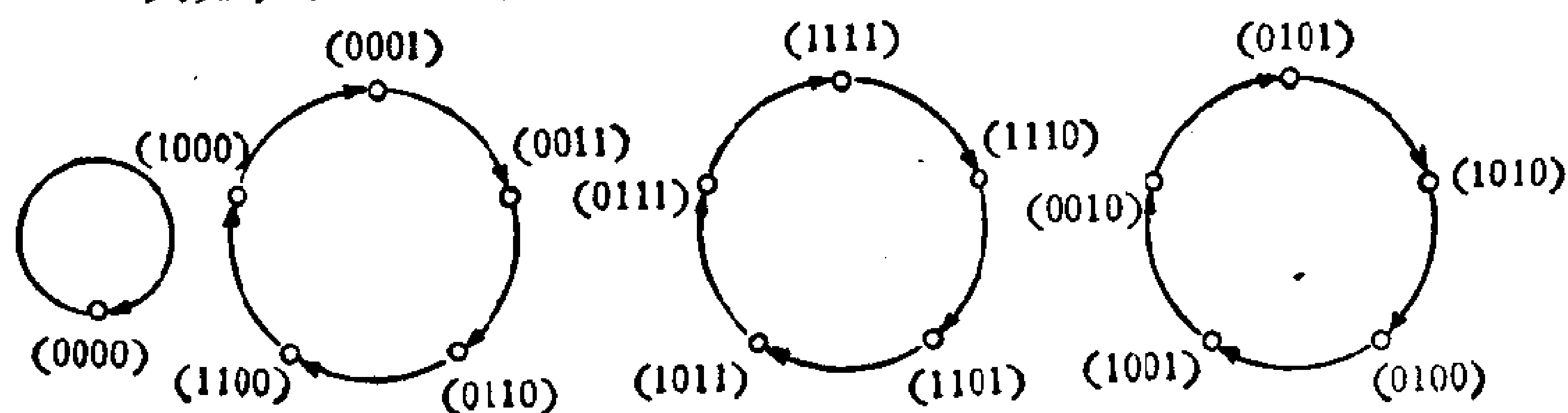


图 1

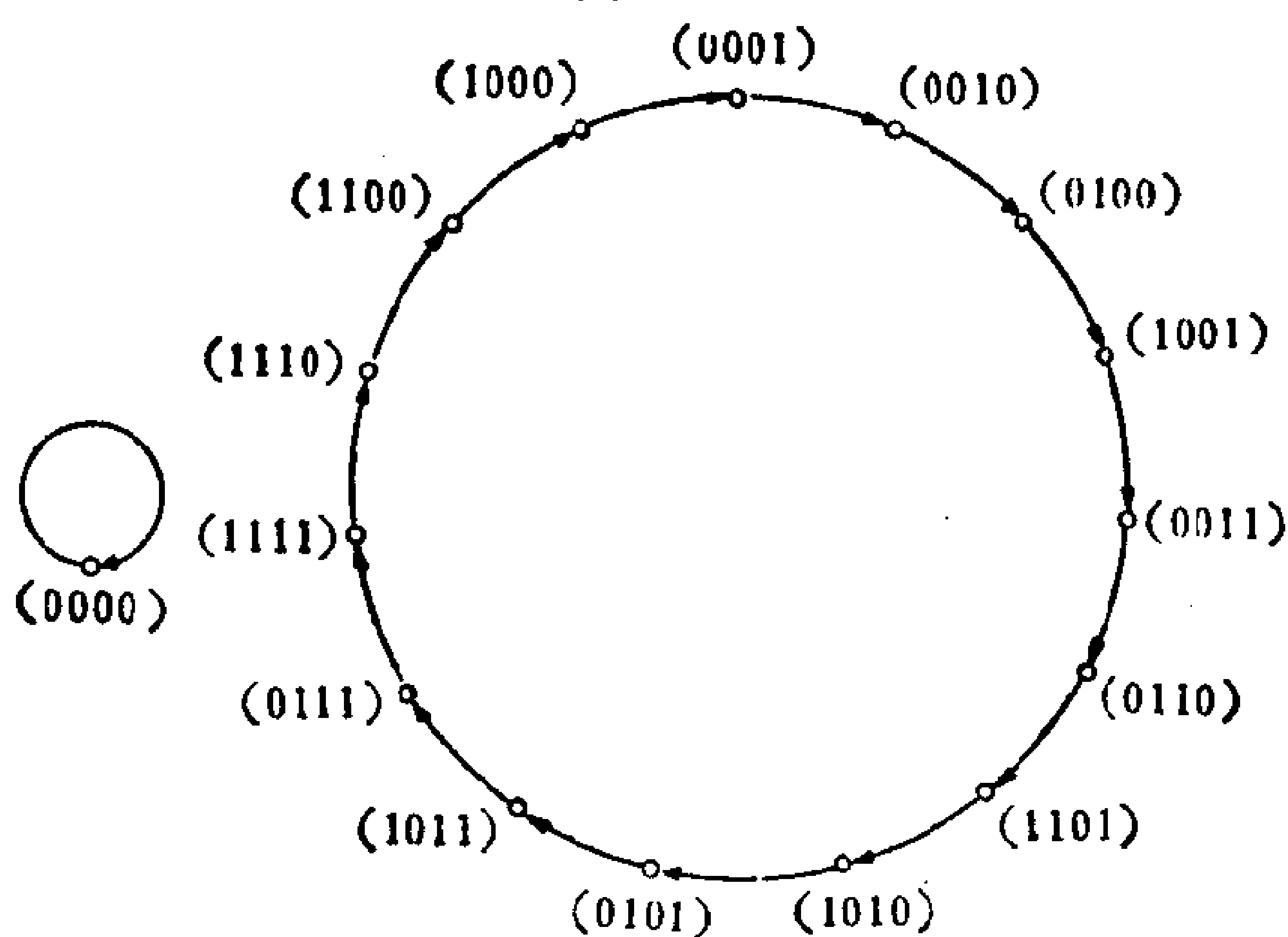


图 2

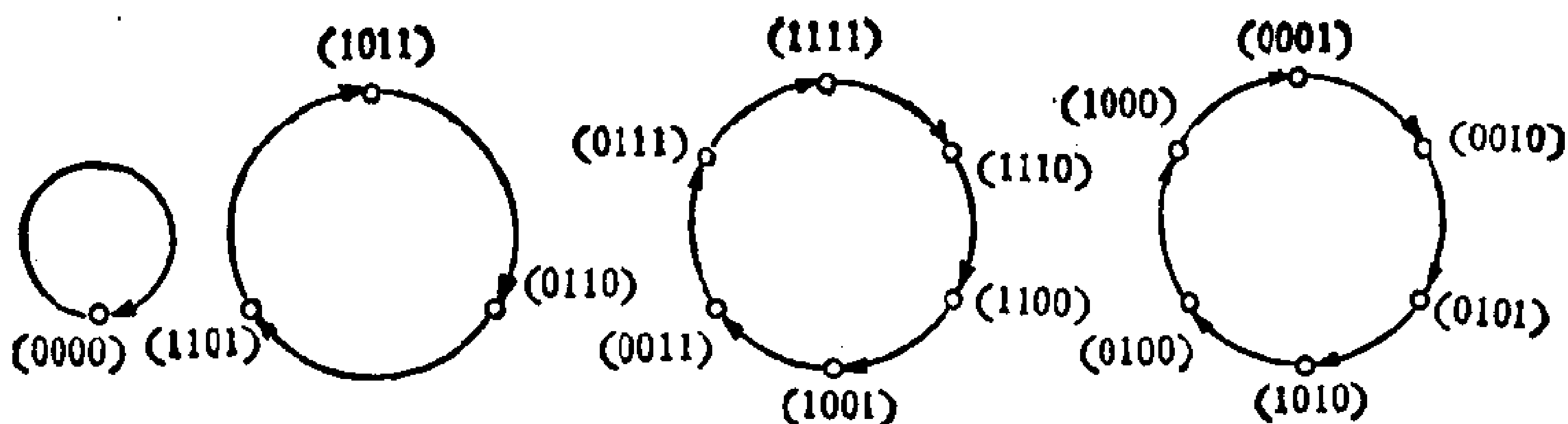


图 3

器的状态图分别是图 1, 图 2 和图 3 中的有向图.

在上面的例子里，状态图都由一些两两无公共顶点的圈组成. 这个事实带有一般性:

定理 5 非退化的 q 元 n 级线性移位寄存器的状态图总是由一些两两无公共顶点的圈组成.

证. 设有一非退化的 q 元 n 级线性移位寄存器，它的联接多项式是零次项等于 1 的一个 n 次多项式 $f(x)$. 根据 §2 定理 1, 从任一初始状态 $(a_0, a_1, \cdots, a_{n-1})$ 出发, 这个移位寄存器都产生一个 q 元周期序列

$$a_0, a_1, a_2, \cdots.$$

设这个周期序列的周期等于 p. 令

$$\mathbf{s}_k=(a_k, a_{k+1}, \cdots, a_{k+(n-1)}), k=0, 1, 2, \cdots,$$

那么状态序列

$$\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \cdots$$

也是个周期等于 p 的序列. 于是 G_f 就有一个圈

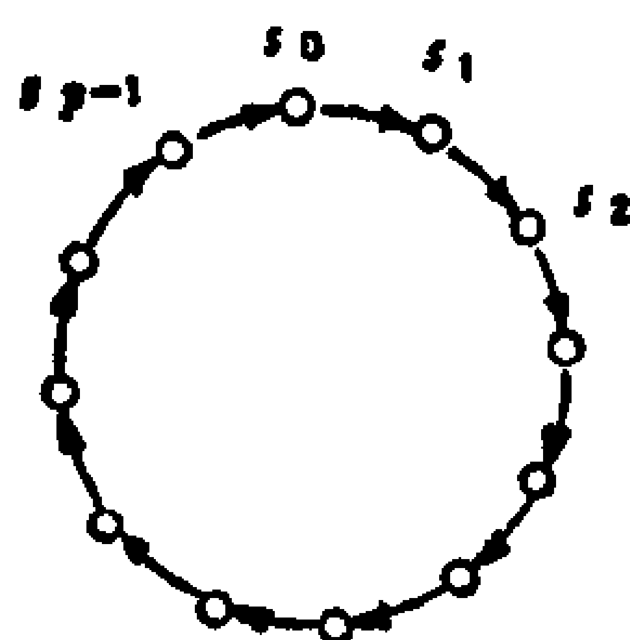


图 4

把这个圈简记作

$$(\mathbf{s}_0,\ \mathbf{s}_1,\ \mathbf{s}_2,\ \cdots,\ \mathbf{s}_{p-1}).$$

这证明 G_f 的任一状态 $(a_0,\ a_1,\ \cdots,\ a_{n-1})$ 都在一个圈上. 又因从 G_f 的任一顶点出发，有且只有一条弧以这个顶点为起点，所以 G_f 的任意两个圈都不可能有公共顶点. 因此 G_f 一定由一些两两没有公共顶点的圈组成.

仍设有一个非退化的 q 元 n 级线性移位寄存器，它的联接多项式是 $f(x)$. 显然它的状态图 G_f 的一个圈上顶点的个数等于这个圈上弧的个数，我们把这个个数叫做这个圈的圈长或圈的周期. 例如零状态 $\mathbf{0}$ 自己组成 G_f 的一个周期等于 0 的圈:

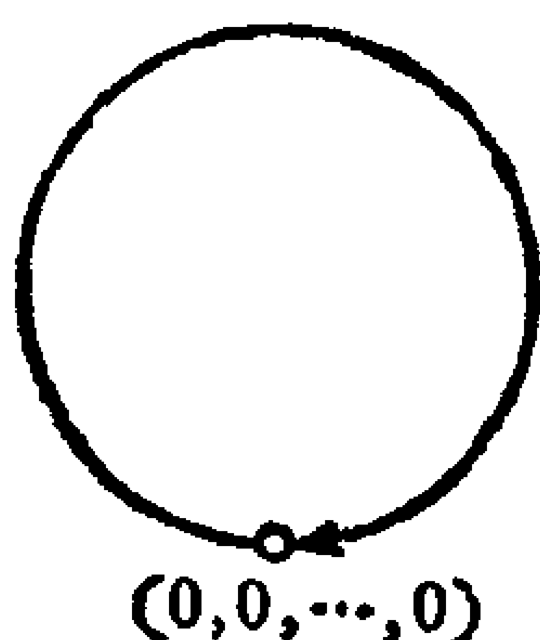


图 5

在定理 5 的证明中实际上也证明了

系理 设有一非退化的 q 元 n 级线性移位寄存器，它的联接多项式是 $f(x)$，那么它产生的任一周期等于 p 的线性移位寄存器序列的连续 p 个状态就构成它的状态图的一个周期等于 p 的圈，特别它的初始状态在一个周期等于 p 的圈上；反过来，如果有一个状态在它的状态图中的一个周期等于 p 的圈上，那么以这个状态为初始状态，这个线性移位寄存器就产生一个周期等于 p 的序列；更进一步，以同一个圈上不同顶点为初始状态所产生的线性移位寄存器序列都平移等价，而且它们组成 $G(f)$ 的一个平移等价类.

又因 $G(f)$ 中任一序列都由它的初始状态所完全确定，所

以也可以用 G_f 中代表它的初始状态的顶点来代表这个序列. 这样, G_f 的一个圈上的顶点就代表 $G(f)$ 的一个平移等价类.

再引进一些形式符号 $[i]$, 其中 i 是正整数. 如果 G_f 由 n_1 个周期等于1的圈, n_2 个周期等于2的圈, $\cdots$, n_i 个周期等于 i 的圈, $\cdots$组成, 那么形式地记

$$\Sigma_f = n_1[1] + n_2[2] + \cdots + n_i[i] + \cdots.$$

注意 Σ_f 这个和是个有限和, 把它叫做 G_f 的圈元. 形式地规定

$$\sum_i n_i[i] + \sum_i m_i[i] = \sum_i (n_i + m_i)[i],$$

$$\left(\sum_i n_i[i]\right) \cdot \left(\sum_i m_j[i]\right) = \sum_{i,j} n_i m_j [i] \cdot [j],$$

其中和都是有限和, 并规定

$$[i] \cdot [j] = (i, j)[[i, j]],$$

其中 (i, j) 和 $[i, j]$ 分别表示 i, j 的最大公因数和最小公倍数.

这样一来, 定理3和定理4可以改述如下:

定理3' 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个零次项等于1的 n 次多项式, 而 $n \geqslant 1$. 并假定

$$f(x) = f_1(x) f_2(x) \cdots f_r(x),$$

其中 $f_i(x)$ 是零次项等于1的 n_i 次多项式, $n_i \geqslant 1$, 而 $f_1(x)$, $f_2(x)$, $\cdots$, $f_r(x)$ 两两互素, 那么

$$\Sigma_f = \Sigma_{f_1} \cdot \Sigma_{f_2} \cdot \cdots \cdot \Sigma_{f_r}.$$

定理4' 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个零次项等于1的 n 次不可约多项式, q 是一个素数 p 的幂, 而 e 是一个正整数, 再设

$$m = \min\{i \mid i \in \mathbf{J} \text{ 而 } p^i \geqslant e\},$$

那么

$$
\begin{aligned}
\Sigma_f = 1[1] &+ \frac{q^n - 1}{p(f)}[p(f)] \\
&+ \sum_{i=1}^{m-1} \frac{q^{np^i} - q^{np^{i-1}}}{p^i p(f)} [p^i p(f)] \\
&+ \frac{q^{n^e} - q^{np^{m-1}}}{p^m p(f)} [p^m p(f)].
\end{aligned}
$$

利用定理 3′ 和定理 4′ 也很容易得到例 2 和例 3 的结果，我们就不重复了.

§4　m 序列和它的采样

我们先重述一下 m 序列的定义.

定义 1　设

$$\mathbf{a} = (a_0,\ a_1,\ a_2,\ \cdots) \tag{1}$$

是一个 q 元 n 级线性移位寄存器序列，它适合线性递归关系式

$$a_k + c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_n a_{k-n} = 0,\ k \geqslant n, \tag{2}$$

其中 $c_n \neq 0$. 如果 $\mathbf{a}$ 的周期是 $q^n - 1$，我们就说 $\mathbf{a}$ 是最长 q 元 n 级线性移位寄存器序列，简称 m 序列.

我们有

定理 1　设有 $\mathbf{F}_q[x]$ 中的多项式

$$f(x) = 1 + \sum_{i=1}^{n} c_i x^i,\ n \geqslant 1,\ \text{而}\ c_n \neq 0. \tag{3}$$

再设 $\mathbf{a}$ 是 $G(f)$ 中的一个非零序列. 如果 $\mathbf{a}$ 是 m 序列，那么 $\mathbf{a}$ 的左移都是 $G(f)$ 中的 m 序列，下面这 $q^n - 1$ 个 m 序列

$$\mathbf{a},\ L(\mathbf{a}),\ L^2(\mathbf{a}),\ \cdots,\ L^{q^n-2}(\mathbf{a}) \tag{4}$$

就是 $G(f)$ 中全部非零序列，而

$$L^{q^n-1}(\mathbf{a}) = \mathbf{a}.$$

更进一步，$\mathbf{a}$ 的状态序列

$$\mathbf{s}_0=(a_0, a_1, a_2, \cdots, a_{n-1}),\ \mathbf{s}_1=(a_1, a_2, a_3, \cdots, a_n),$$
$$\mathbf{s}_2=(a_2, a_3, a_4, \cdots, a_{n+1}), \cdots$$
中 $\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \cdots, \mathbf{s}_{q^n-2}$ 这 q^n-1 个状态就是 $V_n(\mathbf{F}_q)$ 中两两相异的 q^n-1 个非零向量，而 $\mathbf{s}_{q^n-1}=\mathbf{s}_0$.

证. 设 $\mathbf{a}\in G(f)$，即 $\mathbf{a}$ 适合递归关系式 (2)，那么显然 $\mathbf{a}$ 的左移 $L^t(\mathbf{a})$ $(t\geqslant 0)$ 也适合递归关系式 (2)，于是 $L^t(\mathbf{a})\in G(f)$，对 $t\geqslant 0$. 如果 $\mathbf{a}$ 是 m 序列，那么根据 § 3 引理 2 $L^t(\mathbf{a})$ $(t\geqslant 0)$ 都是 m 序列，(4) 中 q^n-1 个 m 序列是 $G(f)$ 中 q^n-1 个两两相异的序列，而 $L^{q^n-1}(\mathbf{a})=\mathbf{a}$. 根据 § 1 定理 1，$|G(f)|=q^n$，因此 (4) 中 q^n-1 个 m 序列就是 $G(f)$ 中全部非零序列.

更进一步，如果 $\mathbf{a}$ 有两个状态 $\mathbf{s}_i$, $\mathbf{s}_j$ 相同，而 $0\leqslant i\leqslant j<q^n-1$，那么一定有 $L^i(\mathbf{a})=L^j(\mathbf{a})$. 因此一定有 $i=j$. 又如果有 $\mathbf{s}_i=(0, 0, \cdots, 0)$，那么由递归关系式推出

$$a_{i+n}=a_{i+n+1}=\cdots=0,$$

因而 $\mathbf{a}$ 是零序列. 所以 $\mathbf{s}_i\neq 0$，对一切 $i\geqslant 0$. 因此 $\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \cdots, \mathbf{s}_{q^n-2}$ 这 q^n-1 个状态就是 $V_n(\mathbf{F}_q)$ 中两两相异的 q^n-1 个非零向量. 因 $L^{q^n-1}(\mathbf{a})=\mathbf{a}$，所以 $\mathbf{s}_{q^n-1}=\mathbf{s}_0$.

定理 1 就证完了.

系理 设 $f(x)=1+\sum\limits_{i=1}^{n} c_i x^i\in\mathbf{F}_q[x]$, $n\geqslant 1$，而 $c_n\neq 0$. 再设 $\mathbf{a}$ 是 $G(f)$ 中的一个非零序列. 如果 $\mathbf{a}$ 是 m 序列，设 $t_1>t_2>0$，那么当 $q^n-1\nmid t_1-t_2$ 时，

$$L^{t_1}(\mathbf{a})+L^{t_2}(\mathbf{a})$$

也是 $G(f)$ 中的 m 序列.

证. 根据定理 1，$L^{t_1}(\mathbf{a}), L^{t_2}(\mathbf{a})\in G(f)$. 再根据 § 1 定理 1，$L^{t_1}(\mathbf{a})+L^{t_2}(\mathbf{a})\in G(f)$. 当 $2^n-1\nmid t_1-t_2$ 时，显然 $L^{t_1}(\mathbf{a})+L^{t_2}(\mathbf{a})\neq\mathbf{0}$，因为否则从 $L^{t_1}(\mathbf{a})+L^{t_2}(\mathbf{a})=\mathbf{0}$ 推出

$L^{t_1-t_2}(\mathbf{a})=\mathbf{a}$. 令 $r=(t_1-t_2)_{q^n-1}$, 那么 $L^r(\mathbf{a})=\mathbf{a}$, 这样 $\mathbf{a}$ 的周期就小于 q^n-1. 这是不可能的. 既然 $L^{t_1}(\mathbf{a})+L^{t_2}(\mathbf{a})\neq 0$, 根据定理 1, 它就是 $G(f)$ 中的 m 序列.

这个系理所证明的关于m序列的性质叫做 m 序列的"移位相加"特性, 它实际上是二元m序列的一个特征性质. 我们有

定理 2 设 $\mathbf{a}$ 是一个周期等于 $p(\mathbf{a})$ 的二元周期序列, 并假定对任意 $i, j(0\leqslant i, j\leqslant p(\mathbf{a})-1)$, $L^i(\mathbf{a})+L^j(\mathbf{a})=\mathbf{0}$ 或 $L^k(\mathbf{a})$, 对某一 $k(0\leqslant k\leqslant p(\mathbf{a})-1)$, 那么 $p(\mathbf{a})=2^n-1$, 对某一 n, 而 $\mathbf{a}$ 是周期 2^n-1 的一个 m 序列.

证. 对任一 $i(0\leqslant i\leqslant p(\mathbf{a})-1)$, 用 $L^i(\mathbf{a})$ 表它的一个周期, 即

$$L^i(\mathbf{a})=(a_i, a_{i+1}, \cdots, a_{p(\mathbf{a})-1}, a_0, a_1, \cdots, a_{i-1}).$$

令
$$V=\mathbf{0}\cup\{L^i(\mathbf{a})\,|\,0\leqslant i\leqslant p(\mathbf{a})-1\},$$

其中 $\mathbf{0}$ 是 $p(\mathbf{a})$ 维零向量. 定理的假设是说 V 是一个交换群. 如果对任意 $(c_0, c_1, c_2, \cdots, c_{p(\mathbf{a})-1})\in V$, $c\in\mathbf{F}_2$, 定义

$$0\cdot(c_0, c_1, c_2, \cdots, c_{p(\mathbf{a})-1})=(0, 0, 0, \cdots, 0),$$

$$1\cdot(c_0, c_1, c_2, \cdots, c_{p(\mathbf{a})}-1)=(c_0, c_1, c_2, \cdots, c_{p(\mathbf{a})-1}),$$

那么 V 就成了 $\mathbf{F}_2$ 上的一个向量空间, 因 V 中元素个数 $p(\mathbf{a})+1$ 有限, 所以 V 是 $\mathbf{F}_2$ 上的有限维向量空间. 设 $\dim V=n$, 那么 $p(\mathbf{a})+1=2^n$, 于是 $p(\mathbf{a})=2^n-1$.

因 $\dim V=n$, 可设 $L^0(\mathbf{a})=\mathbf{a}$, $L^1(\mathbf{a})$, $L^2(\mathbf{a})$, $\cdots$, $L^{r-1}(\mathbf{a})$ 在 $\mathbf{F}_2$ 上线性无关, 而 $L^0(\mathbf{a})$, $L^1(\mathbf{a})$, $L^2(\mathbf{a})$, $\cdots$, $L^{r-1}(\mathbf{a})$, $L^r(\mathbf{a})$ 在 $\mathbf{F}_2$ 上线性相关. 自然 $r\leqslant n$, 那么 $L^r(\mathbf{a})$ 可以表成 $L^0(\mathbf{a})$, $L^1(\mathbf{a})$, $L^2(\mathbf{a})$, $\cdots$, $L^{r-1}(\mathbf{a})$ 的线性组合

$$L^r(\mathbf{a})=c_1L^{r-1}(\mathbf{a})+c_2L^{r-2}(\mathbf{a})+\cdots+c_{r-1}L^1(\mathbf{a})+c_rL^0(\mathbf{a}),\ c_i\in\mathbf{F}_2.$$

将上式作用 $L^{k-r}(k\geqslant r)$, 就得到

$$L^k(\mathbf{a})=c_1L^{k-1}(\mathbf{a})+c_2L^{k-2}(\mathbf{a})+\cdots$$
$$+c_{r-1}L^{k-r+1}(\mathbf{a})+c_rL^{k-r}(\mathbf{a}).$$

上式双方向量的第一分量应该相等，于是就得到

$$a_k=c_1a_{k-1}+c_2a_{k-2}+\cdots$$
$$+c_{r-1}a_{k-r+1}+c_ra_{k-r},\quad k\geqslant r.$$

这就是说 $\mathbf{a}\in G(f)$，而

$$f(x)=1+c_1x+c_2x^2+\cdots+c_rx^r.$$

那么 $L^k(\mathbf{a})\in G(f)$，对任意 $k\geqslant 0$. 于是 $V\subseteq G(f)$. 但 $|G(f)|=2^r$，所以 $n\leqslant r$. 由 $r\leqslant n$ 和 $n\leqslant r$ 推出 $r=n$. 这证明了 $\mathbf{a}$ 是周期 2^n-1 的 m 序列.

我们先给出 m 序列的一个必要条件.

定理 3 设 $f(x)=1+\sum_{i=1}^{n}c_ix^i\in\mathbf{F}_q[x]$，$n\geqslant 1$，而 $c_n\neq 0$. 再设 $\mathbf{a}$ 是 $G(f)$ 中的一个非零序列. 如果 $\mathbf{a}$ 是 m 序列，那么 $f(x)$ 一定是 $\mathbf{F}_q$ 上的不可约多项式.

证. 用反证法. 假定 $f(x)$ 可约，而 $h(x)$ 是 $f(x)$ 的一个不可约因式，即 $h(x)|f(x)$，$h(x)$ 不可约而 $\partial^0h=m<n=\partial^0f$. 因 $h(x)$ 不可约，所以根据 §2 定理 4 的系理 1，$G(h)$ 中任一非零线性移位寄存器序列的周期都等于 $h(x)$ 的周期. 因 $h(x)|f(x)$，故 $G(h)\subset G(f)$. 因此根据定理 1，$G(h)$ 中任一非零序列的周期都等于 q^n-1. 于是 $p(h)=q^n-1$. 但是根据 §2 引理 4，$p(h)|q^m-1$. 因此 $q^n-1|q^m-1$. 但 $m<n$，这是一个矛盾，所以 $f(x)$ 不可约.

我们举一个例子来说明 $f(x)$ 不可约这一条件对于 $G(f)$ 中的非零序列是 m 序列这一点并不充分. 考察 $\mathbf{F}_2$ 上的 4 次多项式

$$f(x)=x^4+x^3+x^2+x+1.$$

因 $\mathbf{F}_2$ 上的一次多项式 x 和 $x+1$ 以及 $\mathbf{F}_2$ 上唯一的二次不可

约多项式 x^2+x+1 都不能整除 $f(x)$，所以 $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式. $f(x)$ 是以下线性递归关系式

$$a_k=a_{k-1}+a_{k-2}+a_{k-3}+a_{k-4},\quad k\geqslant 4$$

的联结多项式. 给了 $G(f)$ 中一个序列的初始状态 (0001)，那么根据 §1 例 1 由上述递归关系式以 (0001) 为初始状态产生的序列是

$$0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\cdots.$$

这个序列的周期是 5，而 $5\neq 2^4-1$，因此它不是 m 序列.

我们回忆，在第一章 §5 定义 2 中定义了 $\mathbf{F}_q$ 上的一个 n 次不可约多项式 $f(x)$ 叫做本原多项式，如果 $f(x)$ 的周期 $p(f)=q^n-1$. 因此 $f(x)$ 是本原多项式，当且仅当 $f(x)$ 的根的公共阶是 q^n-1，也当且仅当

$$q^n-1=\min\{l\,|\,l\in\mathbf{Z},\ l>0,\ 而\ f(x)\,|\,x^l-1\}.$$

我们有

定理 4 设 $f(x)=1+\sum_{i=1}^{n}c_ix^i\in\mathbf{F}_q[x]$，$n\geqslant 1$ 而 $c_n\neq 0$，那么 $G(f)$ 中任一非零序列是 m 序列，当且仅当 $f(x)$ 是本原多项式.

证. 设 $\mathbf{a}$ 是 $G(f)$ 中任一非零序列. 假定 $\mathbf{a}$ 是 m 序列，即 $p(\mathbf{a})=q^n-1$. 根据定理 3，$f(x)$ 不可约. 再根据 §2 定理 4 的系理 1，$p(\mathbf{a})=p(f)$. 所以 $p(f)=q^n-1$. 因此 $f(x)$ 是本原多项式.

反之，设 $f(x)$ 是本原多项式. 再设 $\mathbf{a}$ 是 $G(f)$ 中任一非零序列. 因 $f(x)$ 不可约，根据 §2 定理 4 的系理 1，$p(\mathbf{a})=p(f)$. 因 $f(x)$ 本原，即 $p(f)=q^n-1$. 因此 $p(\mathbf{a})=q^n-1$. 所以 $\mathbf{a}$ 是 m 序列.

这样一来，确定 $\mathbf{F}_q$ 上所有的 m 序列的问题即化为确定 $\mathbf{F}_q$ 上所有的本原多项式这一纯代数问题. 后一问题将在第五

章中讨论.

现在设$f(x)$是$\mathbf{F}_q$上的零次项等于1的n次本原多项式. 根据定理4, $G(f)$中的非零序列都是m序列; 再根据定理1, 它们两两平移等价. 反之, 设$\mathbf{a}$和$\mathbf{b}$是平移等价的n级m序列, 并设$\mathbf{a}\in G(f)$, $\partial^0 f=n$而f的零次项等于1, 那么根据定理4, $f(x)$是$\mathbf{F}_q$上的本原多项式; 再根据定理1, $\mathbf{b}\in G(f)$. 因此$\mathbf{F}_q$上周期为q^n-1的两两平移相异的m序列的个数就等于$\mathbf{F}_q$上零次项等于1的n次本原多项式的个数, 而后者根据第一章§5定理8显然等于$\varphi(q^n-1)/n$. 这证明了

系理 $\mathbf{F}_q$上周期为q^n-1的两两平移相异的m序列的个数等于$\varphi(q^n-1)/n$.

下面我们来讨论m序列的采样.

定义2 设$\mathbf{a}$是$\mathbf{F}_q$上的一个周期序列. 写

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$

再设s是一个正整数, 令

$$\mathbf{a}^{(s)}=(a_0,\ a_s,\ a_{2s},\ \cdots),$$

我们把$\mathbf{a}^{(s)}$叫做$\mathbf{a}$的一个采样, 或$\mathbf{a}$的s采样.

我们要研究q元周期序列$\mathbf{a}$的s采样$\mathbf{a}^{(s)}$与$\mathbf{a}$的关系, 特别m序列的采样与原m序列的关系. 首先我们研究$\mathbf{a}^{(s)}$的周期与$\mathbf{a}$的周期的关系.

引理1 设$\mathbf{a}$是周期为$p(\mathbf{a})$的q元周期序列, 而

$$s\equiv s_1(\operatorname{mod} p(\mathbf{a})),$$

那么

$$\mathbf{a}^{(s)}=\mathbf{a}^{(s_1)}.$$

证. 不仿设$s\geqslant s_1$, 那么可以写

$$s=mp(\mathbf{a})+s_1,\ m\geqslant 0.$$

于是

$$a_{ks}=a_{k(mp(\mathbf{a})+s_1)}=a_{kmp(\mathbf{a})+ks_1}=a_{ks_1},\ \ k\geqslant 0.$$

这就是说

$$\mathbf{a}^{(s)}=\mathbf{a}^{(s_1)}.$$

根据引理1, 在讨论q元周期序列$\mathbf{a}$的s采样时, 只要限

定 $0\leqslant s<p(\mathbf{a})$ 就行了.

引理 2 设 $\mathbf{a}$ 是个周期为 $p(\mathbf{a})$ 的 q 元周期序列，而 s 是任意正整数，那么 $\mathbf{a}^{(s)}$ 也是周期序列，而它的周期是 $\frac{p(\mathbf{a})}{(s, p(\mathbf{a}))}$ 的一个因子.

证. 令
$$l=\frac{p(\mathbf{a})}{(s,\ p(\mathbf{a}))},$$
那么 $p(\mathbf{a})\,|\,ls$. 记 $\mathbf{b}=\mathbf{a}^{(s)}$，那么
$$b_{l+k}=a_{(l+k)s}=a_{ls+ks}=a_{ks}=b_k,\quad k\geqslant 0.$$
因此 $p(\mathbf{b})\,|\,l$，即 $p(\mathbf{a}^s)\,|\,l$.

引理 3 设 $\mathbf{a}$ 是周期为 $p(\mathbf{a})$ 的 q 元周期序列，而 s 是与 $p(\mathbf{a})$ 互素的正整数，那么 $\mathbf{a}^{(s)}$ 也是周期 $p(\mathbf{a})$ 的周期序列.

证. 根据引理 2，$p(\mathbf{a}^{(s)})\,|\,p(\mathbf{a})$. 因 $(s,\ p(\mathbf{a}))=1$，故有正整数 t 存在使
$$st\equiv 1(\mathrm{mod}\, p(\mathbf{a})).$$
显然有
$$\mathbf{a}=\mathbf{a}^{(st)}=(\mathbf{a}^{(s)})^{(t)},$$
仍根据引理 2，$p((\mathbf{a}^{(s)})^{(t)})\,|\,p(\mathbf{a}^{(s)})$，即 $p(\mathbf{a})\,|\,p(\mathbf{a}^{(s)})$. 因此 $p(\mathbf{a}^{(s)})=p(\mathbf{a})$.

为了讨论 m 序列与其采样的关系，我们先给出 m 序列的一个表示法. 我们先定义

定义 3 设 $\mathbf{F}_{q^n}$ 是 q^n 个元素的有限域，它包有 $\mathbf{F}_q$ 作为子域，设 $\xi\in\mathbf{F}_{q^n}$. 定义
$$\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}(\xi)=\xi+\xi^q+\xi^{q^2}+\cdots+\xi^{q^{n-1}},$$
把它叫做 $\mathbf{F}_{q^n}$ 中的元素 ξ 相对于 $\mathbf{F}_q$ 的迹，我们也把 $\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}(\xi)$ 简记作 $\mathrm{Tr}(\xi)$ 或 $\mathrm{Tr}\,\xi$.

引理 4 设 $\mathbf{F}_{q^n}$ 是 q^n 个元素的有限域，而 ξ 是 $\mathbf{F}_{q^n}$ 中任一元素，那么
$$\mathrm{Tr}\,\xi\in\mathbf{F}_q.$$

证. 因 $\xi^{q^n}=\xi$ 对任意 $\xi\in\mathbf{F}_{q^n}$, 所以

$$\begin{aligned}(\mathrm{Tr}\,\xi)^q&=(\xi+\xi^q+\xi^{q^2}+\cdots+\xi^{q^{n-1}})^q\\&=(\xi^q+\xi^{q^2}+\xi^{q^3}+\cdots+\xi^{q^{n-1}}+\xi^{q^n})\\&=\xi+\xi^q+\xi^{q^2}+\cdots+\xi^{q^{n-1}}=\mathrm{Tr}\,\xi.\end{aligned}$$

因 x^q-x 的 q 个根都在 $\mathbf{F}_q$ 中, 而 $\mathrm{Tr}\,\xi$ 是 x^q-x 的根, 所以 $\mathrm{Tr}\xi\in\mathbf{F}_q$.

定理 5 设 $\mathbf{a}$ 是 $\mathbf{F}_q$ 上的一个周期为 q^n-1 的 m 序列, 它的极小多项式 $f(x)$ 是零次项等于 1 的 n 次本原多项式. 再设 $\tilde{f}(x)$ 是与 $f(x)$ 互反的多项式, 并设 α 是 $\tilde{f}(x)$ 的任意一根, 那么总有 $\beta\in\mathbf{F}^*_{q^n}$ 使

$$a_k=\mathrm{Tr}\beta\alpha^k=\sum_{j=0}^{n-1}(\beta\alpha^k)^{q^j},\ \ k\geqslant0.$$

反之, 设 $f(x)$ 是 $\mathbf{F}_q$ 上的零次项等于 1 的 n 次本原多项式, 而 $\tilde{f}(x)$ 是与 $f(x)$ 互反的多项式. 再设 α 是 $\tilde{f}(x)$ 的任意一根, 那么对任意 $\beta\in\mathbf{F}^*_{q^n}$,

$$(\mathrm{Tr}\beta,\ \mathrm{Tr}(\beta\alpha),\ \mathrm{Tr}(\beta\alpha^2),\ \cdots)$$

都是 $G(f)$ 中的 m 序列, 而且这样就得到 $G(f)$ 中全部非零序列.

证. 先设 $\mathbf{a}$ 是 $\mathbf{F}_q$ 上的一个周期为 q^n-1 的 m 序列, 它的极小多项式 $f(x)$ 是本原多项式. 写

$$f(x)=1+\sum_{i=1}^{n}c_ix^i,\ \ c_n\neq0.$$

于是

$$\tilde{f}(x)=x^n+\sum_{i=1}^{n}c_ix^{n-i}$$

也是 n 次本原多项式. 设 α 是 $\tilde{f}(x)$ 的任意一个根, 那么

$$\alpha,\ \alpha^q,\ \alpha^{q^2},\ \cdots,\ \alpha^{q^{n-1}}$$

就是 $\tilde{f}(x)$ 的全部根, 它们都是 $\mathbf{F}_{q^n}$ 的本原元, 而 $\alpha^{q^n}=\alpha$. 从

$$\tilde{f}(\alpha)=\alpha^n+c_1\alpha^{n-1}+c_2\alpha^{n-2}+\cdots+c_n=0$$

推出

$$\alpha^k+c_1\alpha^{k-1}+c_2\alpha^{k-2}+\cdots+c_n\alpha^{k-n}=0,\ \ k\geqslant n.$$

这就是说，序列

$$(1, \alpha, \alpha^2, \alpha^3, \cdots)$$

适合线性递归关系式(2)．因此对任一 $\beta\in\mathbf{F}_{q^n}$，序列

$$(\beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3, \cdots)$$

也适合线性递归关系式 (2)．那么对任一 j, $0\leqslant j\leqslant n-1$，序列

$$(\beta^{q^j}, (\beta\alpha)^{q^j}, (\beta\alpha^2)^{q^j}, (\beta\alpha^3)^{q^j}, \cdots) \tag{5}$$

也适合线性递归关系式 (2)．将 (5) 中序列对 j 求和，而 $j=0, 1, 2, \cdots, n-1$，所得序列

$$(\mathrm{Tr}\beta, \mathrm{Tr}(\beta\alpha), \mathrm{Tr}(\beta\alpha^2), \mathrm{Tr}(\beta\alpha^3), \cdots) \tag{6}$$

自然也适合线性递归关系式 (2)．

但根据引理 4,

$$\mathrm{Tr}(\beta\alpha^k)\in\mathbf{F}_q, \quad k\geqslant 0.$$

因此对任一 $\beta\in\mathbf{F}_{q^n}$，(6)都属于 $G(f)$．当 β 跑过 $\mathbf{F}_{q^n}$ 时，一共得到 q^n 个序列，今证它们两两相异．设有 $\beta_1, \beta_2\in\mathbf{F}_{q^n}$ 使

$$\mathrm{Tr}(\beta_1\alpha^k)=\mathrm{Tr}(\beta_2\alpha^k), \quad k\geqslant 0.$$

记 $\beta_0=\beta_1-\beta_2$，那么从上式推出

$$\mathrm{Tr}(\beta_0\alpha^k)=0, \quad k\geqslant 0.$$

上式中前 n 个式子可写成

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{n-1}} \\ \alpha^2 & (\alpha^2)^q & (\alpha^2)^{q^2} & \cdots & (\alpha^2)^{q^{n-1}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha^{n-1} & (\alpha^{n-1})^q & (\alpha^{n-1})^{q^2} & \cdots & (\alpha^{n-1})^{q^{n-1}} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_0^q \\ \beta_0^{q^2} \\ \vdots \\ \beta_0^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

上式中矩阵的行列式是范德蒙德行列式．因 $\tilde{f}(x)$ 是 n 次本原多项式，所以 α 是 $\mathbf{F}_{q^n}$ 的本原元．因此 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ 两两不同．由第二章 §5 定理 6 推出此矩阵非异．再从第二章 §4 定理 1 推出 $\beta_0=0$，即 $\beta_1-\beta_2=0$．于是 $\beta_1=\beta_2$.

我们证明了，当β跑过$\mathbf{F}_{q^n}$时，一共得到q^n个序列(6)两两相异. 因此它们就是$G(f)$中全部q^n个序列. 当$\beta=0$时，我们得到零序列；而当β跑过$\mathbf{F}_{q^n}^*$时，我们就得到$G(f)$中全部q^n-1个非零序列. 令$\mathbf{a}\in G(f)$，故有$\beta\in\mathbf{F}_{q^n}^*$使(6)就是$\mathbf{a}$. 这就证明了定理5的前半部.

在证明定理5的前半部的过程中实际上也证明了它的后半部.

定理6 设$\mathbf{a}$是$\mathbf{F}_q$上周期为q^n-1的m序列，而$(s, q^n-1)=1$，那么$\mathbf{a}^{(s)}$也是周期为q^n-1的m序列. 更进一步，如果$\mathbf{a}$的极小多项式以γ为其一根，那么$\mathbf{a}^{(s)}$的极小多项式就是以γ^s为其一根的本原多项式.

证. $\mathbf{a}^{(s)}$是周期为q^n-1的周期序列这一点是引理5的直接推论. 问题还要证明$\mathbf{a}^{(s)}$是m序列. 设$f(x)$是$\mathbf{a}$的极小多项式，$\tilde{f}(x)$是与$f(x)$互反的多项式. 再设α是$\tilde{f}(x)$的任意一根，那么有$\beta\in\mathbf{F}_{q^n}^*$使

$$a_k=\operatorname{Tr}(\beta\alpha^k),\quad k\geqslant 0.$$

于是

$$\mathbf{a}^{(s)}=(\operatorname{Tr}\beta,\ \operatorname{Tr}(\beta\alpha^s),\ \operatorname{Tr}(\beta\alpha^{2s}),\ \operatorname{Tr}(\beta\alpha^{3s}),\ \cdots).$$

因$\tilde{f}(x)$是n次本原多项式，所以α是$\mathbf{F}_{q^n}$的本原元. 又因$(s, q^n-1)=1$，所以α^s也是$\mathbf{F}_{q^n}$的本原元. 设α^s在$\mathbf{F}_q$上的极小多项式是$\tilde{f}_s(x)$，而$f_s(x)$是与$\tilde{f}_s(x)$互反的多项式，那么$\tilde{f}_s(x)$，$f_s(x)$都是本原多项式. 根据定理5的后半部知$\mathbf{a}^{(s)}$是$G(f_s)$中周期为q^n-1的m序列.

取$\gamma=\alpha^{-1}$就得到本定理的第二个断言.

系理 设$\mathbf{a}$是$\mathbf{F}_q$上任一给定的周期为q^n-1的m序列，那么$\mathbf{F}_q$上任一周期为q^n-1的m序列皆与$\mathbf{a}$的某一采样平移等价. 更进一步，设$(r, q^n-1)=(s, q^n-1)=1$，那么$\mathbf{a}^{(r)}$和$\mathbf{a}^{(s)}$平移等价，当且仅当$r\equiv s\cdot q^t(\bmod q^n-1)$对某一整数$t$,

而$0\leqslant t\leqslant n-1$.

证. 设 $\mathbf{a}$ 的极小多项式(它当然是本原多项式)以 γ 为一根，那么 γ 是 $\mathbf{F}_{q^n}$ 中的本原元. 再设 $\mathbf{b}$ 是 $\mathbf{F}_q$ 上另一周期为 q^n-1 的 m 序列，那么 $\mathbf{b}$ 的极小多项式的根也是 $\mathbf{F}_{q^n}$ 中的本原元. 可设 γ^s 是 $\mathbf{b}$ 的极小多项式的一个根，而 $(s, q^n-1)=1$. 根据定理 5, $\mathbf{a}^{(s)}$ 是周期为 q^n-1 的 m 序列，而其极小多项式以 γ^s 为一根. 因此 $\mathbf{b}$ 与 $\mathbf{a}^{(s)}$ 有相同的极小多项式，那么根据定理 1, $\mathbf{b}$ 与 $\mathbf{a}^{(s)}$ 平移等价.

又设 $(r, q^n-1)=(s, q^n-1)=1$, 那么 $\mathbf{a}^{(r)}$ 和 $\mathbf{a}^{(s)}$ 的极小多项式分别以 γ^r 和 γ^s 为各自的一根. $\mathbf{a}^{(r)}$ 和 $\mathbf{a}^{(s)}$ 平移等价当且仅当它们有相同的极小多项式，因此当且仅当 γ^r 和 γ^s 是同一本原多项式的根，因而当且仅当 $r\equiv s\cdot q^t \pmod{q^n-1}$对某一整数 t 而 $0\leqslant t\leqslant n-1$.

令 $\quad \mathbf{Z}^*_{q^n-1}=\{a\,|\,1\leqslant a<q^n-1 \text{ 而 } (a, q^n-1)=1\}$.

在 $\mathbf{Z}^*_{q^n-1}$ 中规定了乘法:

$$a\odot b=(ab)_{q^n-1}, \text{ 对任意 } a, b\in\mathbf{Z}^*_{q^n-1}.$$

我们知道 $\mathbf{Z}^*_{q^n-1}$ 对于如上规定的乘法是一个群，而 $|\mathbf{Z}^*_{q^n-1}|=\varphi(q^n-1)$. 容易验证，

$$H=\{1, q, q^2, \cdots, q^{n-1}\}$$

是 $\mathbf{Z}^*_{q^n-1}$ 的一个子群，而 $|H|=n$. $\mathbf{Z}^*_{q^n-1}$ 可唯一地表成 $\dfrac{\varphi(q^n-1)}{n}$ 个 H 的两两相异的陪集的并. 在这 $\dfrac{\varphi(q^n-1)}{n}$ 个 H 的陪集中各选一个代表元:

$$s_1, s_2, \cdots, s_{\varphi(q^n-1)/n}.$$

如果 $\mathbf{a}$ 是 $\mathbf{F}_q$ 上一个周期为 q^n-1 的 m 序列，那么根据定理 5 的系理可知

$$\mathbf{a}^{(s_1)}, \mathbf{a}^{(s_2)}, \cdots, \mathbf{a}^{(s_{\varphi(q^n-1)/n})} \tag{7}$$

就是 $\varphi(q^n-1)/n$ 个两两平移相异的周期为 q^n-1 的 m

序列.

假设我们已经求得 $\mathbf{F}_q$ 上的一个 n 次本原多项式 $f(x)$. 在 $G(f)$ 中选一个非零 m 序列 $\mathbf{a}$. 利用采样的办法就能得到 $\mathbf{F}_q$ 上全部的两两平移相异的周期为 q^n-1 的 m 序列 (7). 如果我们能对 (7) 中每一个 m 序列求出其极小多项式, 那么就求出了 $\mathbf{F}_q$ 上所有的 n 次本原多项式. 下面我们就来讨论如何从一个已知的周期为 q^n-1 的 m 序列去求它的极小多项式这个问题.

我们先证明下面这个引理.

引理 5 设 $\mathbf{a}$ 是 $\mathbf{F}_q$ 上周期等于 q^n-1 的 m 序列, 那么 $\mathbf{a}$ 的任意 n 个连续的状态

$$\mathbf{s}_m,\ \mathbf{s}_{m+1},\ \mathbf{s}_{m+2},\ \cdots,\ \mathbf{s}_{m+n-1},\ m\geqslant 0,$$

在 $\mathbf{F}_q$ 上线性无关, 其中

$$\mathbf{s}_i=(a_i,\ a_{i+1},\ \cdots,\ a_{i+n-1}).$$

证. 设 $\mathbf{a}$ 是由线性递归关系式

$$a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\quad k\geqslant n, \tag{8}$$

所产生的 m 序列, 那么 $c_n\neq 0$, 而

$$f(x)=1+c_1x+c_2x^2+\cdots+c_nx^n$$

是本原多项式. 设有线性关系式

$$d_0\mathbf{s}_m+d_1\mathbf{s}_{m-1}+d_2\mathbf{s}_{m+2}+\cdots+d_{n-1}\mathbf{s}_{m+n-1}=0. \tag{9}$$

因 $\mathbf{a}$ 是 m 序列, 状态

$$\mathbf{s}=(0,\ 0,\ \cdots,\ 0,\ 1)$$

一定在 $\mathbf{a}$ 的状态序列

$$\mathbf{s}_0,\ \mathbf{s}_1,\ \mathbf{s}_2,\ \cdots$$

中出现. 设 $\mathbf{s}=\mathbf{s}_l$. 再设线性递归关系式 (8) 所确定的变换矩阵是 T, T 就是 §1 (11) 式中的矩阵. 将 (9) 式作用 T^{l-m} 之后, 就得到

$$d_0\mathbf{s}+d_1(\mathbf{s}T)+d_2(\mathbf{s}T^2)+\cdots+d_{n-1}(\mathbf{s}T^{n-1})=0.$$

但是
$$\mathbf{s}=(00\cdots001),$$
$$\mathbf{s}T=(00\cdots01*),$$
$$\mathbf{s}T^2=(00\cdots1**),$$
$$\cdots$$
$$\mathbf{s}T^{n-1}=(1*\cdots***).$$
显然 $\mathbf{s}$, $\mathbf{s}T$, $\mathbf{s}T^2$, $\cdots$, $\mathbf{s}T^{n-1}$ 在 $\mathbf{F}_q$ 上线性无关. 因此一定有
$$d_0=d_1=d_2=\cdots=d_{n-1}=0.$$
这证明了引理 5.

设 $\mathbf{a}$ 是 $\mathbf{F}_q$ 上周期为 q^n-1 的 m 序列. 假定它的极小多项式是
$$f(x)=1+c_1x+c_2x^2+\cdots+c_nx^n,$$
那么 $f(x)$ 就是产生 $\mathbf{a}$ 的线性递归关系式
$$a_k=-(c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}),\quad k\geqslant n,$$
的联接多项式, 因而是本原多项式. 问题是如何求出 c_1, c_2, $\cdots$, c_n. 任选 $\mathbf{a}$ 的连续的 $2n$ 项, 譬如
$$a_m,\ a_{m+1},\ a_{m+2},\ \cdots,\ a_{m+2n-1}, \tag{10}$$
那么我们有
$$\left.\begin{aligned} a_{m+n}&=c_1a_{m+n-1}+c_2a_{m+n-2}+\cdots+c_na_m,\\ a_{m+n+1}&=c_1a_{m+n}+c_2a_{m+n-1}+\cdots+c_na_{m+1},\\ &\cdots\\ a_{m+2n-1}&=c_1a_{m+2n-2}+c_2a_{m+2n-3}+\cdots+c_na_{m+n-1}. \end{aligned}\right\} \tag{11}$$
上面这 n 个式子可以看作是 n 个文字 c_1, c_2, $\cdots$, c_n 所适合的 n 个线性方程, 这个线性方程组的系数矩阵是
$$A=\begin{pmatrix} a_{m+n-1} & a_{m+n-2} & \cdots & a_m\\ a_{m+n} & a_{m+n-1} & \cdots & a_{m+1}\\ & \cdots & & \\ a_{m+2n-2} & a_{m+2n-3} & \cdots & a_{m+n-1} \end{pmatrix},$$
将矩阵 A 的每一个行向量的 n 个分量的排列次序颠倒过来,

我们就得到 $\mathbf{a}$ 的 n 个连续的状态

$$\mathbf{s}_m,\ \mathbf{s}_{m+1},\ \cdots,\ \mathbf{s}_{m+n-1}.$$

根据引理5，它们在 $\mathbf{F}_q$ 上线性无关，因此 A 的 n 个行向量线性无关．这就是说 A 是非异的，那么从线性方程组 (11) 可唯一地解出 $c_1,\ c_2,\ \cdots,\ c_n$.

在实际计算中，如果能够取到 $\mathbf{a}$ 的连续 $2n$ 项 (10) 是从 $n-1$ 个 0 开始的 $2n$ 项，即

$$a_m=a_{m+1}=\cdots=a_{m+n-2}=0,\ a_{m+n-1},\ a_{m+n},\ \cdots,\ a_{m+2n-1}$$

那么这时线性方程组 (11) 成为

$$\left.\begin{aligned}a_{m+n}&=c_1a_{m+n-1},\\a_{m+n+1}&=c_1a_{m+n}+c_2a_{m+n-1},\\&\cdots\\a_{m+2n-1}&=c_1a_{m+2n-2}+c_2a_{m+2n-3}+\cdots+c_na_{m+n-1}.\end{aligned}\right\}$$

上述线性方程组的系数矩阵是下三角形矩阵，因此特别容易求解．

更进一步，$c_1,\ c_2,\ \cdots,\ c_n$ 实际上还可以从 m 序列 $\mathbf{a}$ 直接读出，因 $\mathbf{a}$ 是m序列，第 j 个分量是1而其余分量全等于0的状态

$$\mathbf{e}_j=(0\cdots0\underset{\substack{第\\j\\分\\量}}{1}0\cdots0),\ 1\leqslant j\leqslant n,$$

一定在 $\mathbf{a}$ 的状态序列中出现．设

$$\mathbf{s}_{m_j}=\mathbf{e}_j,\ \ 1\leqslant j\leqslant n,$$

那么将 $\mathbf{a}$ 的下面这 $2n$ 个连续的项

$$a_{m_j}=0,\ a_{m_j+1}=0,\ \cdots,\ a_{m_j+j-2}=0,\ a_{m_j+j-1}=1,$$
$$a_{m_j+j}=0,\ \cdots,\ a_{m_j+n-1}=0,\ a_{m_j+n},\ \cdots,\ a_{m_j+2n-1}$$

代入方程组(11)，从第一个方程得到

$$c_{n-j+1}=a_{m_j+n},\ \ 1\leqslant j\leqslant n.$$

§5 m 序列的伪随机性

在这一节里我们着重讨论二元m序列，即假定 $q=2$. 下面我们说到m序列总是指二元m序列.

m序列是很重要的一类二元序列，有着许多重要的应用. 它之所以重要，是因为它有着伪随机性，即它是所谓的伪随机序列. 我们先证明

定理 1 设

$$\mathbf{a}=(a_0, a_1, a_2, \cdots)$$

是 $\mathbf{F}_2$ 上的一个周期为 2^n-1 的m序列. 将 $\mathbf{a}$ 的一个周期

$$(a_0, a_1, a_2, \cdots, a_{2^n-2})$$

依序排列在一个圆周上，并使 a_{2^n-2} 与 a_0 相邻:

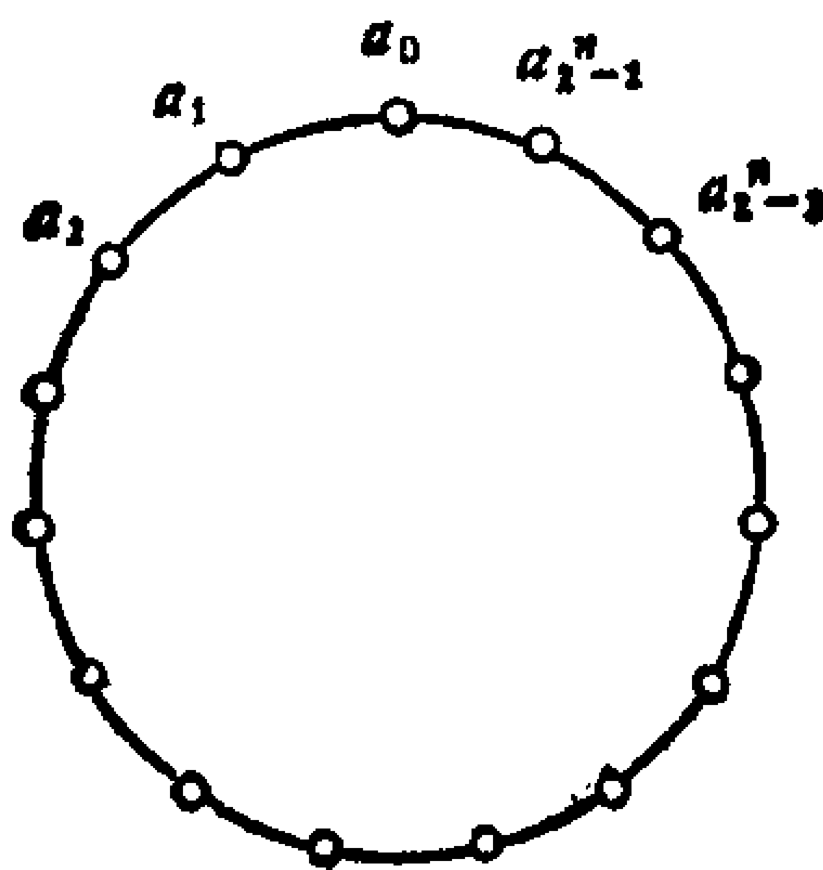


图 1

再设 $0<k\leqslant n$, 那么 $\mathbf{F}_2$ 上任意一个 k 元素组 $(b_1, b_2, \cdots, b_k)$ 在 $\mathbf{a}$ 的一个周期的上述圆周排列中出现的次数等于

$$\begin{cases} 2^{n-k}, & \text{如 } (b_1, b_2, \cdots, b_k)\neq(0, 0, \cdots, 0), \\ 2^{n-k}-1, & \text{如 } (b_1, b_2, \cdots, b_k)=(0, 0, \cdots, 0). \end{cases}$$

证. $\mathbf{F}_2$ 上每个非零 n 元素组是 $\mathbf{a}$ 的一个状态，因而在 $\mathbf{a}$ 的一个周期的上述圆周排列中只出现一次. $\mathbf{F}_2$ 上每个非零 k 元素组的后面任添上 $n-k$ 个 $\mathbf{F}_2$ 中的元素都构成 $\mathbf{a}$ 的一个

状态，因此 $\mathbf{F}_2$ 上每个非零 k 元素组恰出现在 2^{n-k} 个 $\mathbf{a}$ 的状态中作为其前 k 个元素，所以在 $\mathbf{a}$ 的一个周期的上述圆周排列中出现 2^{n-k} 次. $\mathbf{F}_2$ 上的全零 k 元素组 $(0, 0, \cdots, 0)$ 的后面只有添上 $\mathbf{F}_2$ 中 $n-k$ 个不全为 0 的元素时才构成 $\mathbf{a}$ 的一个状态，因此 $\mathbf{F}_2$ 上的全零 k 元素组恰出现在 $2^{n-k}-1$ 个 $\mathbf{a}$ 的状态中作为前 k 个元素，所以在 $\mathbf{a}$ 的一个周期的上述圆周排列中出现 $2^{n-k}-1$ 次.

系理 设 $\mathbf{a}$ 是 $\mathbf{F}_2$ 上周期为 2^n-1 的 m 序列，那么 1 在 $\mathbf{a}$ 的一个周期中恰出现 2^{n-1} 次，而 0 在 $\mathbf{a}$ 的一个周期中恰出现 $2^{n-1}-1$ 次.

下面我们来定义二元周期序列的自相关函数. 令 η 是一个从 $\mathbf{F}_2$ 的加法群到 $+1$ 和 -1 这两个整数所组成的乘法群的同构：

$$\eta(0)=1,\ \eta(1)=-1.$$

我们有

定义 1 设有 $\mathbf{F}_2$ 上的周期序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$

并假定 $\mathbf{a}$ 的周期是 v. $\mathbf{a}$ 的*自相关函数* $c_{\mathbf{a}}(t)$ 是定义在非负整数集合 $\mathbf{Z}$ 上而取整数值的函数：

$$c_{\mathbf{a}}(t)=\sum_{i=0}^{v-1}\eta(a_i)\eta(a_{i+t}),\quad t\in\mathbf{Z}.$$

显然有

$$c_{\mathbf{a}}(0)=v,$$

而

$$c_{\mathbf{a}}(t)\leqslant c_{\mathbf{a}}(0).$$

通常把 $c_{\mathbf{a}}(0)$ 叫做*主峰高度*，而当 $t\not\equiv 0 \pmod v$ 时，把 $|c_{\mathbf{a}}(t)|$ 叫做*副峰高度*.

由于 $\mathbf{a}$ 的周期是 v，显然有

$$c_{\mathbf{a}}(v+k)=c_{\mathbf{a}}(k),\ \text{对一切非负整数}\ k.$$

因此 $c_{\mathbf{a}}(t)$ 由它的连续 v 个函数值，譬如

$$c_{\mathbf{a}}(0),\ c_{\mathbf{a}}(1),\ c_{\mathbf{a}}(2),\ \cdots,\ c_{\mathbf{a}}(v-1)$$

完全确定.

m序列的自相关函数有很理想的性质,这就是

定理 2 设 $\mathbf{a}$ 是 $\mathbf{F}_2$ 上的周期等于 2^n-1 的m序列, 那么

$$c_{\mathbf{a}}(t)=\begin{cases}2^n-1, & \text{如果 } t\equiv 0 \pmod{2^n-1},\\ -1, & \text{如果 } t\not\equiv 0 \pmod{2^n-1}.\end{cases}$$

证. 显然有

$$c_{\mathbf{a}}(0)=2^n-1,$$

因此 $c_{\mathbf{a}}(t)=2^n-1$, 如果 $t\equiv 0 \pmod{2^n-1}$.

以下设 $t\not\equiv 0 \pmod{2^n-1}$.

写 $\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)$,

并设 $f(x)$ 是 $\mathbf{a}$ 的极小多项式, 即 $\mathbf{a}\in G(f)$, 而 $f(x)$ 是 n 次本原多项式. 写

$$f(x)=c_0+c_1x+c_2x^2+\cdots+c_nx^n,\ c_0c_n\neq 0,$$

那么 $\mathbf{a}$ 适合线性递归关系式

$$c_0a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n}=0,\ k\geqslant n. \tag{1}$$

将 $\mathbf{a}$ 左移 t 步所得到的序列

$$L^t(\mathbf{a})=(a_t,\ a_{t+1},\ a_{t+2},\ \cdots),$$

显然也适合(1),那么

$$\mathbf{a}+L^t(\mathbf{a})=(a_0+a_t,\ a_1+a_{t+1},\ a_2+a_{t+2},\ \cdots)$$

也适合(1), 因此也属于 $G(f)$. 但当 $t\not\equiv 0 \pmod{2^n-1}$时, 因 $\mathbf{a}$ 的周期等于 2^n-1, 所以

$$\mathbf{a}+L^t(\mathbf{a})\neq \mathbf{0}.$$

但根据 § 4 定理 1, $G(f)$ 中的非零序列都是m序列, 那么根据定理 1 的系理, 1 在 $\mathbf{a}+L^t(\mathbf{a})$ 的一个周期里出现 2^{n-1} 次, 而 0 在 $\mathbf{a}+L^t(\mathbf{a})$ 的一个周期里出现 $2^{n-1}-1$ 次. 因此

$$c_{\mathbf{a}}(t)=\sum_{i=0}^{2^n-2}\eta(a_i)\eta(a_{i+t})=\sum_{i=0}^{2^n-2}\eta(a_i+a_{i+t})$$
$$=2^{n-1}(-1)+(2^{n-1}-1)\cdot 1=-1.$$

这证明了定理 2.

定理 2 告诉我们，周期为 2^n-1 的 m 序列的自相关函数的主峰高度等于 2^n-1，而副峰高度恒等于 1，因此当 n 大时，主峰高度较副峰高度高很多. m 序列的这一性质是雷达和声纳系统采用 m 序列调制成的信号来测距的根据. 为了阐明 m 序列的这一应用，我们先定义互相关函数的概念.

定义 2 设 $\mathbf{a}$ 和 $\mathbf{b}$ 都是 $\mathbf{F}_2$ 上的周期 v 的周期序列，我们定义它们的互相关函数为

$$c(\mathbf{a},\ \mathbf{b})=\sum_{i=0}^{v-1}\eta(a_i)\eta(b_i).$$

设 $f(x)$ 是 $\mathbf{F}_2$ 上的一个 n 次本原多项式，而 $\mathbf{a}$ 是 $G(f)$ 中一个给定的 m 序列. 再设 $\mathbf{b}$ 是 $G(f)$ 中另一 m 序列. 根据 §3 定理 1，总有非负整数 t_0 存在使 $\mathbf{a}=L^{t_0}(\mathbf{b})$. 问题是怎样很快地算出 t_0. 方法是同时计算

$$c(L^t(\mathbf{b}),\ \mathbf{a}),\ t=0,\ 1,\ 2,\ \cdots,\ 2^n-2.$$

在工程上这可以用相关接收器来完成. 看 $c(L^t(\mathbf{b}),\ \mathbf{a})$ 何时达到主峰高度. 如果当 $t=t_0$ 时，$c(L^{t_0}(\mathbf{b}),\ \mathbf{a})$ 达到主峰高度，那么 $\mathbf{a}=L^{t_0}(\mathbf{b})$.

当用雷达来测量某一目标的距离时，可选用一 m 序列 $\mathbf{a}$ 调制成一串无线电信号，雷达发送这一串信号后，要求它的头一个信号达到目标又折回后不超出 $\mathbf{a}$ 的一个周期，即 $\mathbf{a}$ 的一个周期所调制成的一串信号尚未发送完. 假定 $\mathbf{a}$ 的头一个信号折回时，雷达发送到 $\mathbf{a}$ 的第 t_1 个信号，那么目标的距离就等于

$$t_1Tc/2,$$

其中 T 是产生 m 序列的移位寄存器的一个移位脉冲经历的时间，而 c 是光速. 因此问题是如何求 t_1. 设 $L^{t_1}(\mathbf{a})=\mathbf{b}$. 计算互相关函数

$$c(L^t(\mathbf{b}), \mathbf{a}),\ t=0,\ 1,\ 2,\ \cdots,\ 2^n-2.$$

如果当 $t=t_0$ 时, $c(L^t(\mathbf{b}), \mathbf{a})$ 达到主峰高度,那么

$$t_1=2^n-1-t_0.$$

当然如果 $\mathbf{F}_2$ 上还有其他周期序列也具备定理 2 中所证明的性质, 那么这些周期序列也可用作测距的目的. 为此我们定义

定义 3 设

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)$$

是 $\mathbf{F}_2$ 上的一个周期等于 v 的周期序列. 如果

$$c_{\mathbf{a}}(t)=-1,\quad 对一切\ t\not\equiv 0 \pmod v,$$

我们就说 $\mathbf{a}$ 是个伪随机序列.

有了这个定义,定理 2 可以改述成

定理 2′ m 序列是伪随机序列.

除了 m 序列外, 现在已知的伪随机序列还有二次剩余序列(也叫 L 序列), 孪生素数序列和 Hall 序列. 我们将在 § 7 里介绍它们. 在这里我们先证明伪随机序列的一个简单性质, 这就是

定理 3 设 $\mathbf{a}$ 是个伪随机序列, 那么 $\mathbf{a}$ 的周期 v 一定是个奇数, 而且在 $\mathbf{a}$ 的一个周期里, 1 出现的个数和 0 出现的个数相差 1, 即 1 出现的个数比 0 出现的个数多 1 个或少 1 个.

证. 设

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots,\ a_{v-1},\ a_v,\ \cdots),$$

那么根据定义 2, 有

$$c_{\mathbf{a}}(t)=\begin{cases} v, & 如果\ t=0 \\ -1, & 如果\ 0<t<v. \end{cases}$$

于是

$$\sum_{t=0}^{v-1} c_{\mathbf{a}}(t)=1.$$

另一方面, 根据定义 1,

$$\sum_{t=0}^{v-1} c_{\mathbf{a}}(t) = \sum_{t=0}^{v-1}\sum_{i=0}^{v-1}\eta(a_i)\eta(a_{i+t})$$

$$= \sum_{i=0}^{v-1}\eta(a_i)\sum_{t=0}^{v-1}\eta(a_{i+t})$$

$$= \left(\sum_{i=0}^{v-1}\eta(a_i)\right)^2.$$

因此
$$\left(\sum_{i=0}^{v-1}\eta(a_i)\right)^2 = 1.$$

由此推出
$$\sum_{i=0}^{v-1}\eta(a_i) = 1 \text{ 或 } -1.$$

所以 $\eta(a_0), \eta(a_1), \eta(a_2), \cdots, \eta(a_{v-1})$ 中 1 的个数和 -1 的个数相差 1. 于是 $\mathbf{a}$ 的一个周期里，1 出现的个数和 0 出现的个数相差 1. 由此又推出 $\mathbf{a}$ 的周期 v 一定是奇数.

既然定理 2′ 证明了 m 序列是伪随机序列，所以 m 序列也具有定理 3 中对于伪随机序列所证明的性质. 但这已经在定理 1 的系理中直接证明了.

下面我们再证明 m 序列的另一伪随机性质. 为此我们引进下面这个定义.

定义 4 设 $\mathbf{a}$ 是 $\mathbf{F}_2$ 上的周期为 v 的周期序列. 将 $\mathbf{a}$ 的一个周期

$$(a_0,\ a_1,\ a_2,\ \cdots,\ a_{v-1}) \tag{2}$$

依序排列在一个圆周上使 a_{v-1} 与 a_0 相邻. 我们把这个圆周上形如

$$1\ \underbrace{0\ 0\ 0\ \cdots\ 0}_{\text{都是 } 0}\ 1 \text{ 或 } 0\ \underbrace{1\ 1\ 1\ \cdots\ 1}_{\text{都是 } 1}\ 0$$

的一连串两两相邻的项分别叫做 $\mathbf{a}$ 的一个周期中一个 0 游程或 1 游程. 而 0 游程中 0 的个数和 1 游程中 1 的个数叫做这游程的长.

我们有

定理 4　$\mathbf{F}_2$ 上的周期序列的一个周期中，0 游程的个数等于 1 游程的个数．更进一步，伪随机序列的周期一定 $\equiv 3 \pmod 4$，而周期等于 v 的伪随机序列的一个周期中．0 游程的个数和 1 游程的个数都等于 $(v+1)/4$.

证．设 $\mathbf{a}$ 是 $\mathbf{F}_2$ 上的周期序列，并设 $\mathbf{a}$ 的周期是 v．$\mathbf{a}$ 的一个周期

$$(a_0, a_1, a_2, \cdots, a_{v-1})$$

中，形如　　　　0 1　或　1 0

的相邻的两项分别叫做从 0 到 1 或从 1 到 0 的变化．显然，$\mathbf{a}$ 的一个周期中 0 到 1 的变化的个数等于 1 到 0 的变化的个数．又显然在 $\mathbf{a}$ 的一个周期中，0 游程的个数等于 1 到 0 的变化的个数，而 1 游程的个数等于 0 到 1 的变化的个数．因此 $\mathbf{a}$ 的一个周期中，0 游程的个数等于 1 游程的个数．

更进一步，设 $\mathbf{a}$ 是伪随机序列．用 m 表 $\mathbf{a}$ 的一个周期中 0 游程的个数，那么 $\mathbf{a}$ 的一个周期中 1 游程的个数也是 m．在上一段已经证明，$\mathbf{a}$ 的一个周期中 1 到 0 的变化的个数和 0 到 1 的变化的个数也都是 m．于是

$$\begin{aligned} c_{\mathbf{a}}(1) &= \sum_{i=0}^{v-1} \eta(a_i)\eta(a_{i+1}) \\ &= m(-1\cdot 1) + m(1\cdot -1) + (v-2m) \\ &= v-4m. \end{aligned}$$

因 $\mathbf{a}$ 是伪随机序列，所以又有

$$c_{\mathbf{a}}(1) = -1,$$

因此

$$v-4m = -1.$$

这证明了

$$v \equiv 3 \pmod 4, \quad 而\ m = \frac{v+1}{4}.$$

对于 m 序列，我们有

定理 5　设 $\mathbf{a}$ 是周期等于 2^n-1 的一个 m 序列，那么在 $\mathbf{a}$

的一周期中，游程的总数等于 2^{n-1}，其 0 游程的个数和 1 游程的个数都等于 2^{n-2}．更进一步，长为 $r(0<r<n-1)$ 的 0 游程的个数和 1 游程的个数都等于 2^{n-2-r}；长为 $n-1$ 的 0 游程的个数等于 1，长为 $n-1$ 的 1 游程的个数等于 0；长为 n 的 0 游程的个数等于 0，长为 n 的 1 游程的个数等于 1；长 $>n$ 的游程的个数均等于 0.

证．设 $0<r<n-1$．那么在 **a** 的一个周期中，长为 r 的 0 游程的个数就等于 **a** 中形如

$$1\ \underbrace{0\ 0\ \cdots\ 0}_{r\text{个}0}\ 1\ b_{r+3}\ b_{r+4}\ \cdots\ b_n,\ b_i\in\mathbf{F}_2,$$

的状态的个数．而后者显然等于 2^{n-2-r}．同理，**a** 中长为 r 的 1 游程的个数也等于 2^{n-2-r}.

根据定理 4，**a** 的一个周期中，游程的总数等于

$$2\cdot\frac{2^n-1+1}{4}=2^{n-1}.$$

令
$$2^{n-1}-2\sum_{r=1}^{n-2}2^{n-2-r}=2^{n-1}-\sum_{r=1}^{n-2}2^{n-1-r}=2.$$

因此 **a** 的一个周期中长 $\geqslant n-1$ 的游程只有 2 个．因

$$\underbrace{1\ 1\ \cdots\ 1}_{n\text{个}1}$$

是 **a** 的一个状态，而 **a** 的每个状态在 **a** 的一个周期中恰出现一次，所以这个状态之前的符号与之后的符号都是 0，因此 **a** 恰有 1 个长为 n 的 1 游程：

$$0\ \underbrace{1\ 1\ \cdots\ 1}_{n\text{个}1}\ 0.$$

又因
$$\underbrace{0\ 0\ \cdots\ 0}_{n\text{个}0}$$

不是 **a** 的状态，所以 **a** 不能有长为 n 的 0 游程．又

$$1\underbrace{00\cdots 0}_{n-1\text{个}0}$$

是 $\mathbf{a}$ 的一个状态. 显然这个状态之后的符号必为 1. 这样

$$1\underbrace{00\cdots 0}_{n-1\text{个}0}1$$

就是 $\mathbf{a}$ 中一个长为 $n-1$ 的 0 游程. 由此推出 $\mathbf{a}$ 没有长为 $n-1$ 的 1 游程, 也没有长 $>n$ 的游程.

最后我们来解释一下伪随机序列名称的由来, 当掷一枚均匀的分币时, 若出现国徽面我们就记一个 1, 若出现分值面我们就记一个0. 如果掷的次数足够多时, 譬如掷 n 次后, 我们就记下来一个随机的二元序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1}),$$

它具有下面三条随机特性:

1) 序列中 1 的个数和 0 的个数接近相等.

2) 序列的自相关函数

$$c_{\mathbf{a}}(t)=\sum_{i=0}^{n} a_i a_{i+t}$$

当 $t=0$ 时最高, 而当 $t\neq 0$ 时迅速下降.

3) 把连在一起的 1 (或 0) 称为游程, 其中 1 (或 0) 的个数称为此游程的长度. $\mathbf{a}$ 中长为 1 的游程约占游程总数的 1/2, 长为 2 的游程约占游程总数的 $1/2^2$, 长为 3 的游程约占游程总数的 $1/2^3$, …. 在同样长度的所有游程中, 1 游程和 0 游程大致各占一半.

这三条特性是真正的二元随机序列的特性. 而前面定义 3 中定义的伪随机序列则具有性质 1 和 2. 我们加上个"伪"字, 是因为这些序列虽然表面上满足伪随机特性 1) 和 2), 但实际上它们却是按一定规律形成的序列. 伪随机序列常被用来在保密通信中起加密作用和在自动控制系统的识辨中模拟

随机噪声．今扼要介绍如下：

设有一二元数字信息序列

$$c_0,\ c_1,\ c_2,\ \cdots \tag{3}$$

在发送之前，我们选定一个伪随机序列对它进行加密．设

$$a_0,\ a_1,\ a_2,\ \cdots \tag{4}$$

是一个伪随机序列．我们将(3)和(4)这两个序列按项相加，得到加密后的信息序列

$$c_0+a_0,\ c_1+a_1,\ c_2+a_2,\ \cdots \tag{5}$$

我们发送的就是(5)．当收信者收到信息序列(5)之后，再将(5)与选定的伪随机序列(4)按项相加，这就是解密，结果重新得到二元数字信息序列(3)．当然也可以选定任意一个线性移位寄存器序列来对(3)进行加密．

m 序列实际上就是一个很好的二电平的伪随机噪声序列．为了得到 n 电平的序列，我们选一个 n 级的 m 序列，即周期等于 2^n-1 的 m 序列(4)．我们有状态序列

$$\mathbf{s}_0,\ \mathbf{s}_1,\ \mathbf{s}_2,\ \cdots$$

其中 $\qquad \mathbf{s}_k=(a_k,\ a_{k+1},\ a_{k+2},\ \cdots,\ a_{k+n-1}),\ \ k\geqslant 0.$

将 $a_i(i=0,\ 1,\ 2,\ \cdots)$ 都看作整数，令

$$b_k=a_k+a_{k+1}+a_{k+2}+\cdots+a_{k+n-1},\ \ k\geqslant 0,$$

那么我们就得到一个 n 电平的序列

$$b_0,\ b_1,\ b_2,\ \cdots, \tag{6}$$

根据定理1，在(4)的一个周期里，每个非零二元 n 元素组都出现一次而只出现一次．因此任一整数 m $(1\leqslant m\leqslant n)$ 在(6)的连续 2^n-1 项中出现的次数是组合数

$$\binom{n}{m}.$$

§6 m 序列的互相关函数

在这一节里，我们仍然假定 $q=2$. 我们要讨论周期相等的两个m序列的互相关函数，并给出一个求多个周期相等的 m 序列（其互相关函数的绝对值与自相关函数的主峰相比较小）的一个算法. 在具体推导过程中，要用到第四章的结果；特别是第四章§3 的定理 4 和§5 的定理 1. 因此对本节所讨论的问题有兴趣的读者，顶好先读完第四章§5 以后，再回来读本节. 我们先给出下面的定义.

定义 1 设 $\mathbf{a}$, $\mathbf{b}$ 是周期 v 的二元序列. 写

$$\begin{aligned}\mathbf{a}&=(a_0,\ a_1,\ a_2,\ \cdots),\\ \mathbf{b}&=(b_0,\ b_1,\ b_2,\ \cdots),\end{aligned}\qquad a_i,\ b_i\in\mathbf{F}_2.$$

设 τ 是个非负整数. 定义 $\mathbf{a}$ 和 $\mathbf{b}$ 的互相关函数为

$$c_{\mathbf{a},\mathbf{b}}(\tau)=\sum_{i=0}^{v-1}\eta(a_i)\eta(b_{i+\tau}),\tag{1}$$

其中 η 是从 $\mathbf{F}_2$ 的加法群到 $+1$ 和 -1 组成的乘法群的同构映射:

$$\eta(0)=1,\ \eta(1)=-1.$$

利用作用在二元周期序列上的左移变换 L, 可将互相关函数(1)表成

$$c_{\mathbf{a},\mathbf{b}}(\tau)=c_{\mathbf{a},L^{\tau}(\mathbf{b})}(0).$$

上一节所定义的周期 v 的二元序列 $\mathbf{a}$ 的自相关函数 $c_{\mathbf{a}}(\tau)$ 实际上就是

$$c_{\mathbf{a}}(\tau)=c_{\mathbf{a},\mathbf{a}}(\tau).$$

特别，当 $\mathbf{a}$ 是周期 2^n-1 的m序列时，我们有

$$c_{\mathbf{a}}(\tau)=\begin{cases}2^n-1, & 如果\ \tau\equiv0(\bmod 2^n-1),\\ -1, & 如果\ \tau\not\equiv0(\bmod 2^n-1).\end{cases}$$

先研究由 $\mathbf{F}_2$ 上同一个 n 次本原多项式 $f(x)$ 所产生的两个 m 序列 $\mathbf{a}$ 和 $\mathbf{b}$ 的互相关函数．这时，$\mathbf{a}$，$\mathbf{b}\in G(f)$．因此根据 § 4 定理 1 有非负整数 t 存在使 $\mathbf{b}=L^t(\mathbf{a})$．于是

$$
\begin{aligned}
c_{\mathbf{a},\mathbf{b}}(\tau)&=c_{\mathbf{a},L^t(\mathbf{a})}(\tau)=c_{\mathbf{a},\mathbf{a}}(t+\tau)=c_{\mathbf{a}}(t+\tau)\\
&=\begin{cases}2^n-1, & \text{如果 } t+\tau\equiv 0(\operatorname{mod} 2^n-1),\\ -1, & \text{如果 } t+\tau\not\equiv 0(\operatorname{mod} 2^n-1).\end{cases}
\end{aligned}
$$

因此这时问题特别简单．下面我们着重讨论由 $\mathbf{F}_2$ 上不同的 n 次本原多项式所产生的 m 序列的互相关函数．

设 α 是 2^n 个元素的有限域 $\mathbf{F}_{2^n}$ 的一个本原元．设 $f(x)$ 是 $\mathbf{F}_2$ 上的一个 n_0 次不可约多项式，而 $n_0|n$，那么 $f(x)$ 的根都属于 $\mathbf{F}_{2^n}$．于是 $f(x)$ 的 n_0 个根都是 α 的幂，设为

$$\alpha^{i_1},\ \alpha^{i_2},\ \cdots,\ \alpha^{i_{n_0}}.$$

不妨假定 $$0<i_1<i_2<\cdots<i_{n_0}<2^n-1.$$

这时我们说 α^{i_1} 是 $f(x)$ 的首根．注意，首根当然是相对于本原元 α 来说的．以下我们总选定 $\mathbf{F}_{2^n}$ 的一个本原元 α．

下面这个引理要用到第四章中的结果．

引理 1 设 α 是 $\mathbf{F}_{2^n}$ 的一个本原元．用 $f_i(x)$ 表示 α^i 的极小多项式．设 $1<d<2^n-1$．令

$$g_{d-1}=\frac{x^{2^n-1}-1}{[f_1, f_2, \cdots, f_{d-1}]},$$

其中 $[f_1, f_2, \cdots, f_{d-1}]$ 表示 $f_1, f_2, \cdots, f_{d-1}$ 的最低公倍式，那么对任意 $\mathbf{a}$，$\mathbf{b}\in G(g_{d-1})$，我们有

$$|c_{\mathbf{a},\mathbf{b}}(0)|\leqslant 2^n-1-2d.$$

证．根据第四章 § 3 定理 4，$G(g_{d-1})$ 中序列的前 2^n-1 项组成一个循环码 $C(g_{d-1})$，它的生成多项式是 $[f_1, f_2, \cdots, f_{d-1}]$．再根据第四章 § 5 可知，$C(g_{d-1})$ 是设计距离 d 的本原 BCH 码．根据第四章 § 5 定理 1 可知，对任意 $\mathbf{a}$，$\mathbf{b}\in C(g_{d-1})$，它们的 Hamming 距离 $\rho(\mathbf{a}, \mathbf{b})\geqslant d$．注意，$c_{\mathbf{a},\mathbf{b}}(0)$ 是 $\mathbf{a}$，$\mathbf{b}$

中相应位置的码元相等的个数减去相应位置的码元不等的个数. $\mathbf{a}, \mathbf{b}$ 中相应位置的码元不等的个数等于 $\mathbf{a}-\mathbf{b}$ 的 Hamming 重量 $w(\mathbf{a}-\mathbf{b})$. 但 $w(\mathbf{a}-\mathbf{b})=\rho(\mathbf{a}, \mathbf{b})$. 所以

$$c_{\mathbf{a},\mathbf{b}}(0)=2^n-1-2\rho(\mathbf{a}, \mathbf{b})\leqslant 2^n-1-2d. \tag{2}$$

另一方面,显然有 $x-1|g_{d-1}$, 那么全 1 序列 $(1, 1, 1, \cdots)$ 属于 $G(g_{d-1})$. 因此 2^n-1 维全 1 向量

$$\mathbf{1}=\underbrace{(1, 1, \cdots, 1)}_{2^n-1\text{个}1}$$

属于 $C(g_{d-1})$. 于是 $\mathbf{1}+\mathbf{b}\in C(g_{d-1})$, 那么也有 $\rho(\mathbf{a}, \mathbf{1}+\mathbf{b})\geqslant d$ 根据和上面同样的道理,有

$$c_{\mathbf{a},\mathbf{1}+\mathbf{b}}(0)\leqslant 2^n-1-2d.$$

但 $$c_{\mathbf{a},\mathbf{1}+\mathbf{b}}(0)=\sum_{i=0}^{2^n-2}\eta(a_i)\eta(1+b_i)=\sum_{i=0}^{2^n-2}\eta(a_i)\cdot-\eta(b_i)$$

$$=-\sum_{i=0}^{2^n-2}\eta(a_i)\eta(b_i)=-c_{\mathbf{a},\mathbf{b}}(0).$$

因此

$$c_{\mathbf{a},\mathbf{b}}(0)\geqslant-(2^n-1-2d). \tag{3}$$

于是由(2), (3)两式推出

$$|c_{\mathbf{a},\mathbf{b}}(0)|\leqslant 2^n-1-2d.$$

这样就证明了引理 1.

定理 1 设 α 是 $\mathbf{F}_{2^n}$ 的一个本原元,

$$\alpha^{u_1}, \alpha^{u_2}, \cdots, \alpha^{u_k}(0<i<2^n-1)$$

分别是 $\mathbf{F}_2$ 上 n 次本原多项式 $f_{u_1}(x), f_{u_2}(x), \cdots, f_{u_k}(x)$ 的首根. 假定

$$u_1>u_2>\cdots>u_k,$$

那么对任意 $\mathbf{a}_i\in G(f_{u_i}), \mathbf{a}_j\in G(f_{u_j}), i\neq j$, 我们有

$$|c_{\mathbf{a}_i,\mathbf{a}_j}(\tau)|\leqslant 2^n-1-2u_k.$$

证. 显然有

$$f_{u_i}(x)\,|\,g_{u_k-1}(x),\ 1\leqslant i\leqslant k.$$

因此 $\mathbf{a}_i$, $\mathbf{a}_j\in G(g_{u_k-1})$ $(1\leqslant i, j\leqslant k)$. 于是 $L^\tau(\mathbf{a}_j)\in G(g_{u_k-1})$. 当 $i\neq j$ 时,根据引理1就有

$$|c_{\mathbf{a}_i,\mathbf{a}_j}(\tau)|=|c_{\mathbf{a}_i,L^\tau(\mathbf{a}_j)}(0)|\leqslant 2^n-1-2u_k.$$

这证明了定理1.

从定理1可知，要求互相关函数的绝对值与自相关函数的主峰相比较小的多个m序列，只要选 $\mathbf{F}_{2^n}$ 的本原元 α 的一些可作为 n 次本原多项式首根的幂: α^{u_1}, α^{u_2}, $\cdots$, α^{u_k}, $u_1>u_2>\cdots>u_k$, 而 u_k 尽可能地大即可. 先研究 α^m 何时是 n 次本原多项式的首根. 显然必须有 $(m, 2^n-1)=1$; 但仅仅这一条件是不够的.

引理2 设 α 是 $\mathbf{F}_{2^n}$ 的一个本原元. 如果 α^m 是 $\mathbf{F}_2$ 上 n_0 次不可约多项式$f(x)$ 的一个根, 那么 α^m, $\alpha^{m\cdot 2}$, $\alpha^{m\cdot 2^2}$, $\cdots$ 都是 $f(x)$ 的根, 而 α^m, $\alpha^{m\cdot 2}$, $\alpha^{m\cdot 2^2}$, $\cdots$, $\alpha^{m2^{n_0-1}}$ 就是$f(x)$ 的全部 n_0 个两两不同的根.

证. 这个引理实际上在第一章§5定理7中已经证明了.

现在设m是个正整数, $0<m<2^n-1$. 将m表成二进位数

$$m=m_{n-1}\cdot 2^{n-1}+m_{n-2}\cdot 2^{n-2}+\cdots$$
$$+m_1\cdot 2+m_0,\quad m_i=0 \text{ 或 } 1.$$

这样m就确定了一个二元n维非零行向量

$$\mathbf{m}=(m_{n-1},\ m_{n-2},\ \cdots,\ m_1,\ m_0).$$

反过来, 设 $(m_{n-1}, m_{n-2}, \cdots, m_1, m_0)$ 是个二元n维非零行向量,那么它就确定一个正整数

$$m=m_{n-1}\cdot 2^{n-1}+m_{n-2}\cdot 2^{n-2}+\cdots+m_1\cdot 2+m_0,$$

而 $0<m<2^n-1$.

设 $\mathbf{m}=(m_{n-1}, m_{n-2}, \cdots, m_1, m_0)$ 是个二元n维非零行向量. 它里面形状

$$(\underbrace{00\cdots0}_{\text{全是}0}1 \quad 或 \quad 1\underbrace{00\cdots0}_{\text{全是}0}1 \quad 或 \quad 1\underbrace{00\cdots0}_{\text{全是}0})$$

的连续几个项叫做一个 0 游程，0 的个数叫做 0 游程的长．它里面形状

$$(\underbrace{11\cdots1}_{\text{全是}1}0 \quad 或 \quad 0\underbrace{11\cdots1}_{\text{全是}1}0 \quad 或 \quad 0\underbrace{11\cdots1}_{\text{全是}1})$$

的连续几个项叫做一个 1 游程，1 的个数叫做 1 游程的长．

例如，$n=11$ 时，(01101110111) 中有三个 0 游程，它们的长都等于 1；有三个 1 游程，一个的长等于 2，两个的长等于 3．又如 (01111011111) 中有两个 0 游程，它们的长都等于 1；有两个 1 游程，一个的长等于 4，一个的长等于 5．

我们先证明

引理 3 设 α 是 $\mathbf{F}_{2^n}$ 的一个本原元，而 $0<m<2^n-1$．如果 α^m 是它所适合的 $\mathbf{F}_2$ 上的极小多项式 $f(x)$ 的首根，那么 m 所确定的二元 n 维非零行向量 $\mathbf{m}=(m_{n-1}, m_{n-2}, \cdots, m_1, m_0)$ 一定从 0 开始而以 1 结束，即 $m_{n-1}=0$, $m_0=1$．

证．因 $0<m<2^n-1$，$\mathbf{m}$ 一定有一个分量不等于 0．设 $\mathbf{m}$ 的等于 0 的分量中足码最大的一个是 l，即

$$m_{n-1}=m_{n-2}=\cdots=m_{l+1}=1$$

而 $m_l=0$．根据引理 2，$\alpha^{m\cdot 2^{n-l-1}}$ 也是 $f(x)$ 的根．显然 $(m\cdot 2^{n-l-1})_{2^n-1}$ 确定的二元 n 维行向量是

$$(m_l, m_{l-1}, \cdots, m_1, m_0, m_{n-1}, m_{n-2}, \cdots, m_{l+1}).$$

因 α^m 是 $f(x)$ 的首根，$m\leqslant(m\cdot 2^{n-l-1})_{2^n-1}$．所以 $m_{n-1}\leqslant m_l=0$．于是 $n-1=l$．因此 $m_{n-1}=0$．

其次，设 $m_0=0$．根据引理 2，$\alpha^{m\cdot 2^{n-1}}$ 也是 $f(x)$ 的根．显然 $(m\cdot 2^{n-1})_{2^n-1}$ 确定的二元 n 维行向量是

$$(m_0, m_{n-1}, m_{n-2}, \cdots, m_2, m_1).$$

因 α^m 是 $f(x)$ 的首根，$m\leqslant(m\cdot 2^{n-1})_{2^n-1}$．于是 $m_{n-1}\leqslant m_0$，

$m_{n-2} \leqslant m_{n-1}$, $m_{n-3} \leqslant m_{n-2}$, $\cdots$ 从 $m_{n-2} \leqslant m_{n-1} = 0$ 推出 $m_{n-2} = 0$. 从 $m_{n-3} \leqslant m_{n-2}$ 推出 $m_{n-3} = 0$. 如此继续下去,就有 $m_{n-1} = m_{n-2} = \cdots = m_1 = m_0 = 0$. 这就是说 $m=0$, 这与 $0<m<2^n-1$ 的假设相矛盾. 这样就证明了引理3.

仍设 α 是 $\mathbf{F}_{2^n}$ 的一个本原元, 而 $0<m<2^n-1$, 并假定 α^m 是它所适合的 $\mathbf{F}_2$ 上的极小多项式 $f(x)$ 的首根, 那么根据引理3, m 所确定的二元 n 维非零行向量 $\mathbf{m}$ 从0开始而以1结束, 那么从左向右数, $\mathbf{m}$ 的第一个游程是0游程, 最末一个游程是1游程, 而 $\mathbf{m}$ 一共有偶数个游程. 设 $\mathbf{m}$ 一共有 $2s$ 个游程, s 是个正整数. 并假定从左向右数, $\mathbf{m}$ 的第 $2i-1$ 个游程的长等于 r_i, 而 $\mathbf{m}$ 的第 $2i$ 个游程的长等于 $t_i (1 \leqslant i \leqslant s)$, 那么 $\mathbf{m}$ 就确定了 $2s$ 个正整数 $r_1, t_1, r_2, t_2, \cdots, r_s, t_s$, 而 $\sum_{i=1}^{s}(r_i+t_i) = n$. 于是

$$\mathbf{m} = (\underbrace{0, \cdots, 0}_{r_1\text{个}0}, \underbrace{1, \cdots, 1}_{t_1\text{个}1}, \underbrace{0, \cdots, 0}_{r_2\text{个}0}, \underbrace{1, \cdots, 1}_{t_2\text{个}1}, \cdots, \underbrace{0, \cdots, 0}_{r_s\text{个}0}, \underbrace{1, \cdots, 1}_{r_s\text{个}1}).$$

仿照引理3的证明, 可以更进一步证明

引理4 设 α 是 $\mathbf{F}_{2^n}$ 的一个本原元, 而 $0<m<2^n-1$. 假定 m 所确定的二元 n 维非零行向量 $\mathbf{m}$ 是

$$\mathbf{m} = (\underbrace{0, \cdots, 0}_{r_1\text{个}0}, \underbrace{1, \cdots, 1}_{t_1\text{个}1}, \underbrace{0, \cdots, 0}_{r_2\text{个}0}, \underbrace{1, \cdots, 1}_{t_2\text{个}1}, \cdots, \underbrace{0, \cdots, 0}_{r_s\text{个}0}, \underbrace{1, \cdots, 1}_{t_s\text{个}1}),$$

而 $\sum_{i=1}^{s}(r_i+t_i) = n$. 那么 α^m 是它所适合的 $\mathbf{F}_2$ 上的极小多项式的首根, 当且仅当以下两个条件之一成立:

1) $r_1 = r_2 = \cdots = r_s$ 而且 $t_1 = t_2 = \cdots = t_s$.

2) 对任一 $\geqslant 2$ 而 $\leqslant s$ 的正整数 $i(2\leqslant i\leqslant s)$，存在一个正整数 l，(l 依赖于 i)$0<l\leqslant s$，使得

$$r_1=r_i,\ t_1=t_i,\ r_2=r_{i+1},\ t_2=t_{i+1},\ \cdots,\ r_{l-1}=r_{i+l-2},$$
$$t_{l-1}=t_{i+l-2},\ r_l>r_{i+l-1}$$

或

$$r_1=r_i,\ t_1=t_i,\ r_2=r_{i+1},\ t_2=t_{i+1},\ \cdots,\ r_{l-1}=r_{i+l-2},$$
$$t_{l-1}=t_{i+l-2},\ r_l=r_{i+l-1},\ t_l<t_{i+l-1},$$

这里当 r 和 t 的足码 $k>s$ 时，均理解为用 s 去除 k 所得的余数 $(k)_s$.

由于这个引理的证明在原则上和引理 3 完全一样，因此我们就不写出来了.

根据引理 3 和引理 4，我们可以写出一个算法，用这个算法可以求出 $\mathbf{F}_{2^n}$ 的本原元 α 的一些可以作为 n 次本原多项式首根的幂: α^{u_1}, α^{u_2}, $\cdots$, α^{u_k}, $u_1>u_2>\cdots>u_k$，而 u_k 尽可能大.

(1) 列出适当多个相应的正整数 m 尽可能大的，从 0 开始而以 1 结束的，适合引理 4 中条件 1) 或条件 2) 的二元非零 n 维行向量 $\mathbf{m}$.

1.1) 先列出相应的正整数是最大的一个，即

$$(0\ \underbrace{1\ 1\ \cdots\ 1}_{n-1\text{个}1}).$$

1.2) 再列出相应的正整数是次大的一个；当 n 是奇数时，即是

$$(0\ \underbrace{1\ 1\ \cdots\ 1}_{\frac{n-3}{2}\text{个}1}\ 0\ \underbrace{1\ 1\ \cdots\ 1}_{\frac{n-1}{2}\text{个}1});$$

而当 n 是偶数时，即是

$$(0\ \underbrace{1\ 1\ \cdots\ 1}_{\frac{n-2}{2}\text{个}1}\ 0\ \underbrace{1\ 1\ \cdots\ 1}_{\frac{n-2}{2}\text{个}1}).$$

1.3) 再列出相应的正整数是第三大的一个；当 n 是奇数

时，即是

$$(0\underbrace{1\ 1\ \cdots\ 1}_{\frac{n-5}{2}\text{个}1}0\underbrace{1\ 1\ \cdots\ 1}_{\frac{n+1}{2}\text{个}1});$$

而当 n 是偶数时，即是

$$(0\underbrace{1\ 1\ \cdots\ 1}_{\frac{n-4}{2}\text{个}1}0\underbrace{1\ 1\ \cdots\ 1}_{\frac{n}{2}\text{个}1}).$$

1.4) 等等.

(2) 将(1)中列出的二元 n 维非零行向量相应的正整数按大小为序排好:

$$u_{1'}>u_{2'}>\cdots>u_{m'}.$$

(3) 将 $u_{1'}, u_{2'}, \cdots, u_{m'}$ 中与 2^n-1 不互素的那些删去. 设剩下的是

$$u_1>u_2>\cdots>u_k.$$

(4) $\alpha^{u_1}, \alpha^{u_2}, \cdots, \alpha^{u_k}$ 就都是 n 次本原多项式的首根.

现在假定 $\mathbf{a}$ 是周期为 2^n-1 的 m 序列，不妨假定 $\mathbf{a}$ 由 $\mathbf{F}_2$ 上的 n 次本原多项式 $f(x)$ 产生，而 α 是 $f(x)$ 的一个根，那么根据 §4 定理 6, $\mathbf{a}^{(u_1)}, \mathbf{a}^{(u_2)}, \cdots, \mathbf{a}^{(u_k)}$ 分别由 $\alpha^{u_1}, \alpha^{u_2}, \cdots, \alpha^{u_k}$ 在 $\mathbf{F}_2$ 上极小多项式所产生. 因 $\alpha^{u_1}, \alpha^{u_2}, \cdots, \alpha^{u_k}$ 都是 n 次本原多项式的首根，所以 $\mathbf{a}^{(u_1)}, \mathbf{a}^{(u_2)}, \cdots, \mathbf{a}^{(u_k)}$ 两两不平移等价，于是有

(5) $\mathbf{a}^{(u_1)}, \mathbf{a}^{(u_2)}, \cdots, \mathbf{a}^{(u_k)}$ 都是周期 2^n-1 的 m 序列，而且分别由 $\mathbf{F}_2$ 上 k 个两两不同的本原多项式产生. 根据定理 1, 它们的互相关函数的绝对值

$$|c_{\mathbf{a}^{(u_i)},\mathbf{a}^{(u_j)}}(\tau)|\leqslant 2^n-1-2u_k,$$

对 $1\leqslant i, j\leqslant k$ 而 $i\neq j$.

实际上, (1)—(5) 就给出了求互相关函数的绝对值仅可能小的适当多个周期相等的m序列的一个算法. 当 n 不太大

时，这个算法用手算并不复杂．当然，如要求出 $\mathbf{a}^{(u_1)}, \mathbf{a}^{(u_2)}, \cdots, \mathbf{a}^{(u_s)}$ 的极小多项式，可利用 §4 的末尾所介绍的算法或后面 §8 中介绍的算法．

下面我们举几个例子来说明上面介绍的算法．

例1 $n=9$, $2^9-1=511=7\cdot73$. 依序列出

$$(0\,1\,1\,1\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,1\,0\,1\,1\,1\,1),$$
$$(0\,1\,1\,0\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,0\,1\,1\,0\,1\,1).$$

它们相应的正整数分别是

$$u_1=2^8-1=255, \qquad u_2=255-2^4=239,$$
$$u_3=239-2^5+2^4=223, \quad u_4=223-2^2=219.$$

它们都和 2^9-1 互素，而

$$2^9-1-2\cdot u_2=33,\ 2^9-1-2\cdot u_3=65,$$
$$2^9-1-2\cdot u_4=73.$$

例2 $n=11$, $2^{11}-1=2047=23\times89$. 依序列出

$$(0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,1\,0\,1\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,0\,1\,1\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1).$$

它们相应的正整数依序是

$$u_1=2^{10}-1=1023, \qquad u_2=1023-2^5=991,$$
$$u_3=991-2^6+2^5=959, \quad u_4=959-2^7+2^6=895,$$
$$u_5=895-2^3=887.$$

它们都和 $2^{11}-1$ 互素，而

$$2^{11}-1-2\cdot u_3=129,\ 2^{11}-1-2\cdot u_4=257,$$
$$2^{11}-1-2\cdot u_5=273.$$

例 3 $n=13$, $2^{13}-1=8191$. 依序列出

$$(0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,1\,1\,1\,0\,1\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,1\,0\,1\,1\,1\,1\,1\,1\,1\,1),$$
$$(0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1\,1),$$
$$(0\,1\,1\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1).$$

它们相应的正整数依序是

$$u_1=2^{12}-1=4095, \qquad u_2=4095-2^6=4031,$$
$$u_3=4031-2^7+2^6=3967, \qquad u_4=3967-2^8+2^7=3839,$$
$$u_5=3839-2^4=3823, \qquad u_6=3839-2^9+2^8=3583.$$

它们都与 $2^{13}-1$ 互素, 而

$$2^{13}-1-2u_3=257, \qquad 2^{13}-1-2u_4=513,$$
$$2^{13}-1-2u_5=545, \qquad 2^{13}-1-2u_6=1015.$$

基于上面的算法, 定理 1 有下面这个特例, 即戈尔德 (Gold) 的优选对:

定理 2 设 α 是 $\mathbf{F}_{2^n}$ 的一个本原元. 令

$$u_1=2^{n-1}-1$$

$$u_2=\begin{cases}2^{n-1}-2^{(n-1)/2}-1, & \text{如果 } 2\nmid n,\\ 2^{n-1}-2^{n/2}-1, & \text{如果 } 2\mid n \text{ 而 } 4\nmid n.\end{cases}$$

那么对任意 $\mathbf{a}\in G(f_{u_1})$, $\mathbf{b}\in G(f_{u_2})$, $\tau\geqslant 0$, 我们有

$$|c_{\mathbf{a},\mathbf{b}}(\tau)|\leqslant\begin{cases}2^{(n+1)/2}+1, & \text{如果 } 2\nmid n,\\ 2^{(n+2)/2}+1, & \text{如果 } 2\mid n \text{ 而 } 4\nmid n.\end{cases}$$

证. 首先注意, 相应于

$$(0\ \underbrace{1\ 1\cdots 1}_{n-1\text{个}1})$$

的正整数是 $2^{n-1}-1$；而当 n 是奇数时，相应于

$$(0\underbrace{1\ 1\cdots 1}_{\frac{n-3}{2}\text{个}1}0\underbrace{1\ 1\cdots 1}_{\frac{n-1}{2}\text{个}1})$$

的正整数是 $2^{n-1}-2^{(n-1)/2}-1$，当 n 是偶数时，相应于

$$(0\underbrace{1\ 1\cdots 1}_{\frac{n-4}{2}\text{个}1}0\underbrace{1\ 1\cdots 1}_{\frac{n}{2}\text{个}1})$$

的正整数是 $2^{n-1}-2^{n/2}-1$. 因此 α^{u_1} 和 α^{u_2} 都分别是它们的极小多项式的首项. 更进一步，容易证明：

$$(2^n-1,\ 2^{n-1}-1)=1,$$

$$(2^n-1,\ 2^{n-1}-2^{(n-1)/2}-1)=1,\quad \text{如果 } 2\nmid n,$$

$$(2^n-1,\ 2^{n-1}-2^{n/2}-1)=1,\quad \text{如果 } 2\mid n \text{ 而 } 4\nmid n.$$

因此 α^{u_1} 和 α^{u_2} 都分别是它们所适合的本原多项式的首根. 那么根据定理 1，对任意 $\mathbf{a}\in G(f_{u_1})$，$\mathbf{b}\in G(f_{u_2})$，$\tau\geqslant 0$，有

$$|c_{\mathbf{a},\mathbf{b}}(\tau)|\leqslant 2^n-1-2u_2$$

$$=\begin{cases}2^n-1-2(2^{n-1}-2^{(n-1)/2}-1)=2^{(n+1)/2}+1, & \text{如果 } 2\nmid n,\\ 2^n-1-2(2^{n-1}-2^{n/2}-1)=2^{(n+2)/2}+1, & \text{如果 } 2\mid n \text{ 而 } 4\nmid n.\end{cases}$$

这就证明了定理 2.

从定理 2 可以推出戈尔德优选组：

定理 3 设 α 是 $\mathbf{F}_{2^n}$ 的一个本原元，选 u_1 和 u_2 如定理 2，并假定 $f_{u_1}(x)$ 和 $f_{u_2}(x)$ 分别是 α^{u_1} 和 α^{u_2} 所适合的 n 次本原多项式，那么 $G(f_{u_1}\cdot f_{u_2})$ 中的非零序列的周期都等于 2^n-1，它们分到 2^n+1 个平移等价类里，对 $G(f_{u_1}\cdot f_{u_2})$ 中任一非零序列 $\mathbf{a}$：

$$|c_{\mathbf{a},\mathbf{a}}(\tau)|\leqslant\begin{cases}2^{(n+1)/2}+1, & \text{如果 } 2\nmid n,\\ 2^{(n+2)/2}+1, & \text{如果 } 2\mid n \text{ 而 } 4\nmid n;\end{cases}$$

而对 $G(f_{u_1}\cdot f_{u_2})$ 中任意两个平移不等价的序列 $\mathbf{a}$，$\mathbf{b}$：

$$|c_{\mathbf{a},\mathbf{b}}(\tau)|\leqslant\begin{cases}2^{(n+1)/2}+1, & \text{如果 } 2\nmid n,\\ 2^{(n+2)/2}+1, & \text{如果 } 2\mid n \text{ 而 } 4\nmid n.\end{cases}$$

证. 因 f_{u_1} 和 f_{u_2} 都是本原多项式，而它们有不同的首根，所以 $(f_{u_1}\cdot f_{u_2})=1$. 因此根据 § 3 定理 1, 我们有

$$G(f_{u_1}\cdot f_{u_2})=G(f_{u_1})\dot{+}G(f_{u_2}).$$

那么 $G(f_{u_1}\cdot f_{u_2})$ 中任一非零序列 $\mathbf{a}$ 可唯一地表成

$$\mathbf{a}=\mathbf{a}_1+\mathbf{a}_2,\ \mathbf{a}_i\in G(f_{u_i}),$$

而 $\mathbf{a}_1$, $\mathbf{a}_2$ 不全为零序列. 用 $p(\mathbf{a})$, $p(\mathbf{a}_1)$, $p(\mathbf{a}_2)$ 表 $\mathbf{a}$, $\mathbf{a}_1$, $\mathbf{a}_2$ 的周期，根据 § 3 定理 2,

$$p(\mathbf{a})=[p(\mathbf{a}_1),\ p(\mathbf{a}_2)]=2^n-1.$$

这证明了 $G(f_{u_1}\cdot f_{u_2})$中任一非零序列的周期都等于 2^n-1. 又因 $\partial^0(f_{u_1}\cdot f_{u_2})=2n$, 所以 $G(f_{u_1}\cdot f_{u_2})$ 中一共有 $2^{2n}-1$ 个非零序列. 因此 $G(f_{u_1}\cdot f_{u_2})$ 中的非零序列分到 $(2^{2n}-1)/(2^n-1)=2^n+1$ 个平移等价类里.

对 $G(f_{u_1}\cdot f_{u_2})$ 中任一非零序列 $\mathbf{a}$, 仍设 $\mathbf{a}=\mathbf{a}_1+\mathbf{a}_2$, $\mathbf{a}_i\in G(f_{u_i})$. 写

$$\mathbf{a}_i=(a_{i0},\ a_{i1},\ a_{i2},\ \cdots),\ i=1,\ 2,$$

那么

$$\begin{aligned}c_{\mathbf{a},\mathbf{a}}(\tau)&=\sum_{j=0}^{2^n-2}\eta(a_{1j}+a_{2j})\eta(a_{1j+\tau}+a_{2j+\tau})\\&=\sum_{j=0}^{2^n-2}\eta(a_{1j})\eta(a_{2j})\eta(a_{1j+\tau})\eta(a_{2j+\tau})\\&=\sum_{j=0}^{2^n-2}\eta(a_{1j}+a_{1j+\tau})\eta(a_{2j}+a_{2j+\tau})\\&=c_{\mathbf{a}_1+L^\tau(\mathbf{a}_1),\,\mathbf{a}_2+L^\tau(\mathbf{a}_2)}(0).\end{aligned}$$

因 $\mathbf{a}_1+L^\tau(\mathbf{a}_1)\in G(f_{u_1})$, $\mathbf{a}_2+L^\tau(\mathbf{a}_2)\in G(f_{u_2})$, 所以根据定理 1 有

$$|c_{\mathbf{a}_1+L^\tau(\mathbf{a}_1),\,\mathbf{a}_2+L^\tau(\mathbf{a}_2)}(0)|\leqslant 2^n-1-2u_2,$$

因此

$$|c_{\mathbf{a},\mathbf{a}}(\tau)|=|c_{\mathbf{a}_1+L^\tau(\mathbf{a}_1),\mathbf{a}_2+L^\tau(\mathbf{a}_2)}(0)|$$
$$=\begin{cases}2^{(n+1)/2}+1, & \text{如果 } 2\nmid n,\\ 2^{(n+2)/2}+1, & \text{如果 } 2|n \text{ 而 } 4\nmid n.\end{cases}$$

对 $G(f_{u_1}\cdot f_{u_2})$ 中任意两个平移不等价的序列 $\mathbf{a}$, $\mathbf{b}$, 设

$$\mathbf{a}=\mathbf{a}_1+\mathbf{a}_2,\ \mathbf{a}_i\in G(f_{u_i}),$$
$$\mathbf{b}=\mathbf{b}_1+\mathbf{b}_2,\ \mathbf{b}_i\in G(f_{u_i}).$$

写
$$\mathbf{a}_i=(a_{i0},\ a_{i1},\ a_{i2},\ \cdots),i=1,\ 2,$$
$$\mathbf{b}_i=(b_{i0},\ b_{i1},\ b_{i2},\ \cdots),i=1,\ 2.$$

那么
$$c_{\mathbf{a},\mathbf{b}}(\tau)=\sum_{j=0}^{2^n-2}\eta(a_{1j}+a_{2j})\eta(b_{1j+\tau}+b_{2j+\tau})$$
$$=\sum_{j=0}^{2^n-2}\eta(a_{1j})\eta(a_{2j})\eta(b_{1j+\tau})\eta(b_{2j+\tau})$$
$$=\sum_{j=0}^{2^n-2}\eta(a_{1j}+b_{1j+\tau})\eta(a_{2j}+b_{2j+\tau})$$
$$=c_{\mathbf{a}_1+L^\tau(\mathbf{b}_1),\mathbf{a}_2+L^\tau(\mathbf{b}_2)}(0).$$

因 $\mathbf{a}_1,\mathbf{b}_1\in G(f_{u_1}),\mathbf{a}_2,\mathbf{b}_2\in G(f_{u_2})$, 所以 $\mathbf{a}_1+L^\tau(\mathbf{b}_1)\in G(f_{u_1})$, $\mathbf{a}_2+L^\tau(\mathbf{b}_2)\in G(f_{u_2})$. 那么根据定理 1 有

$$|c_{\mathbf{a}_1+L^\tau(\mathbf{b}_1),\mathbf{a}_2+L^\tau(\mathbf{b}_2)}(0)|\leqslant 2^n-1-2u_2.$$

因此
$$|c_{\mathbf{a},\mathbf{b}}(\tau)|=|c_{\mathbf{a}_1+L^\tau(\mathbf{b}_1),\mathbf{a}_2+L^\tau(\mathbf{b}_2)}(0)|$$
$$=\begin{cases}2^{(n+1)/2}+1, & \text{如果 } 2\nmid n,\\ 2^{(n+2)/2}+1, & \text{如果 } 2|n \text{ 而 } 4\nmid n.\end{cases}$$

这样定理 3 就完全证明了.

§7 其他伪随机序列

前面我们讨论的二元序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)$$

都是它的项(或元素) $a_i=0$ 或 1 的序列, 这是因为让 $a_i(i=0,1,2,\cdots)$ 在 $\mathbf{F}_2$ 中取值, 对于讨论线性移位寄存器序列比较

方便. 但在讨论二元周期序列的自相关函数时，我们采用了一个将 $\mathbf{F}_2$ 的加法群映到 $+1$ 和 -1 这两个实数所组成的乘法群的同构 η，即我们先把 $\mathbf{F}_2$ 上的一个二元序列经 η 映成一个元素是 $+1$ 或 -1 的序列之后，再来定义它的自相关函数. 因此我们有时也把二元序列看成是元素等于 $+1$ 或 -1 的序列，这在讨论二元周期序列的自相关函数时比较方便. 在这一节里，我们说到二元序列总是指元素等于 $+1$ 或 -1 的序列，我们先重述一下自相关函数和伪随机序列的定义.

定义 1 设

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),\ \ a_i=+1\text{ 或 }-1,$$

是个周期等于 v 的二元序列，我们定义 $\mathbf{a}$ 的自相关函数 $c_{\mathbf{a}}(t)$ 为

$$c_{\mathbf{a}}(t)=\sum_{i=0}^{v-1}a_i a_{i+t},\ t=0,\ 1,\ 2,\ \cdots.$$

我们说 $\mathbf{a}$ 是伪随机序列，如果

$$c_{\mathbf{a}}(t)=\begin{cases} v, & \text{如果 } t\equiv 0 \pmod v, \\ -1, & \text{如果 } t\not\equiv 0 \pmod v. \end{cases}$$

根据前一节的讨论我们知道：伪随机序列的周期 v 一定是 $\equiv 3 \pmod 4$ 的奇数，在它的一个周期里 $+1$ 出现的次数和 -1 出现的次数相差 1，而且在它的一个周期里 $+1$ 游程的个数和 -1 游程的个数都等于$\dfrac{v+1}{4}$.

我们也知道，m 序列都是伪随机序列.

下面我们要介绍另一些伪随机序列，但我们只介绍这些序列的定义，而略去它们是伪随机序列的证明. 读者如果想知道这些证明. 请参看本书后面所附参考书 [22] 中的第十一章.

首先我们来介绍二次剩余序列，它也叫勒让德(Legendre)

序列，或简称L序列.

设p是一个奇素数，再设a是一个与p互素的整数. 我们说a是$\bmod p$的二次剩余，如果同余式

$$x^2 \equiv a \pmod p$$

有整数解x；否则a就叫$\bmod p$的二次非剩余. 引进勒让德(Legendre)符号

$$\left(\frac{a}{p}\right)=\begin{cases}+1, & \text{如果 } a \text{ 是 } \bmod p \text{ 的二次剩余,}\\ -1, & \text{如果 } a \text{ 是 } \bmod p \text{ 的二次非剩余,}\end{cases}$$

并规定
$$\left(\frac{mp}{p}\right)=+1, \text{ 对任意整数 } m.$$

特别
$$\left(\frac{0}{p}\right)=+1.$$

我们得到一个二元序列

$$\left(\frac{0}{p}\right),\ \left(\frac{1}{p}\right),\ \left(\frac{2}{p}\right),\ \cdots. \tag{1}$$

显然，当$(a, p)=1$时，a和$a+p$同时是$\bmod p$的二次剩余或二次非剩余，因此

$$\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right), \text{ 对一切 } a\geqslant 0.$$

这就是说(1)是周期等于p的二元序列. 我们把(1)叫做*二次剩余序列，或勒让德序列，简称L序列*.

可以证明，当p是形状$4t-1$(t是正整数)的素数时，周期等于p的L序列是伪随机序列. 但当p是形状$4t+1$(t是正整数)的素数时，周期等于p的L序列的自相关函数取p, 1, -3三个值，因此这时的L序列不是伪随机序列.

我们再作一个注记. 因为对任意整数k，都有

$$(x+kp)^2 \equiv x^2 \pmod p,$$

所以要检查一个整数$a(0<a<p)$是不是$\bmod p$的二次剩余只要检查a是不是在集合

$$\{(1^2)_p,\ (2^2)_p,\ \cdots,\ ((p-1)^2)_p\}$$

中出现就行了．更进一步，因为

$$x^2\equiv(p-x)^2 (\bmod p),$$

所以要检查一个整数 $a(0<a<p)$ 是不是 $\bmod p$ 的二次剩余只要检查 a 是不是在集合

$$\left\{(1^2)_p,\ (2^2)_p,\ \cdots,\ \left(\left(\frac{p-1}{2}\right)^2\right)_p\right\}$$

中出现就行了．

我们举几个例子．先看 $p=7=4\cdot2-1$ 的情形．这时

$1^2\equiv1(\bmod 7)$，$2^2\equiv4(\bmod 7)$，$3^2\equiv2(\bmod 7)$．

因此 1, 2, 4 是 mod 7 的二次剩余；3, 5, 6 是 mod 7 的二次非剩余，这样我们可以写出周期等于 7 的 L 序列：

$$+1+1+1-1+1-1-1\cdots$$

容易直接验证这是个伪随机序列．

再看 $p=11=4\cdot3-1$ 的情形．这时

$1^2\equiv1(\bmod 11)$，$2^2\equiv4(\bmod 11)$，$3^2\equiv9(\bmod 11)$

$4^2\equiv5(\bmod 11)$，$5^2\equiv3(\bmod 11)$．

因此 1, 3, 4, 5, 9 是 mod 11 的二次剩余；2, 6, 7, 8, 10 是 mod 11 的二次非剩余，我们可以写出周期等于 11 的 L 序列的一个周期

$$+1\ +1\ -1\ +1\ +1\ +1\ -1\ -1\ -1\ +1\ -1$$

可以直接验证它也是个伪随机序列．

再看 $p=19=4\cdot5-1$ 的情形．这时

$1^2\equiv1(\bmod 19)$，$2^2\equiv4(\bmod 19)$，$3^2\equiv9(\bmod 19)$，

$4^2=16(\bmod 19)$，$5^2=6(\bmod 19)$，$6^2\equiv17(\bmod 19)$，

$7^2=11(\bmod 19)$，$8^2\equiv7(\bmod 19)$，$9^2\equiv5(\bmod 19)$．

因此 1, 4, 5, 6, 7, 9, 11, 16, 17 是 mod 19 的二次剩余，而 2, 3, 8, 10, 12, 13, 14, 15, 18 是 mod 19 的二次非剩余．我

们得到一个周期 19 的 L 序列的一个周期

$$+1\ +1\ -1\ -1\ +1\quad +1\ +1\ +1\ -1\ +1$$
$$-1\ +1\ -1\ -1\ -1\quad -1\ +1\ +1\ -1$$

它也是个伪随机序列.

还可以证明周期 $p=3$ 和 7 的 L 序列也是 m 序列，但以其他的 $p=2^n-1(n>3)$ 为周期的 L 序列却都不是 m 序列.

还应该指出形状是 $4t-1$ 的素数的个数比形状是 2^n-1 的整数要多得多. 例如，周期小于 100 的，是伪随机序列的 L 序列的周期，可以是 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83；而周期小于 100 的 m 序列的周期只有 3, 7, 15, 31, 63. 周期愈大，两个相邻的 m 序列的周期的距离愈来愈大，如周期在 100 与 1000 之间的 m 序列的周期只有 127, 255, 511；相对比之下，是伪随机序列的 L 序列的周期就多得多.

但是另一方面，m 序列很容易产生，即可以用线性移位寄存器产生. 无论是用软件(即程序)或硬件(电子设备)来产生 L 序列都比 m 序列复杂. 根据 L 序列的定义和前面所作的注记，可以写出产生 L 序列的算法，这个算法是可以编成程序的.

产生 L 序列的算法 设 p 是一个素数.

(1) 依序计算

$$(1^2)_p,\ (2^2)_p,\ \cdots,\ \left(\left(\frac{p-1}{2}\right)^2\right)_p.$$

(2) 令 $a_0=+1$. 依序查找 $i=1, 2, \cdots, p-1$ 是否在第 (1) 步算出的 $(p-1)/2$ 个数中出现. 如果出现，就令 $a_i=+1$；如果不出现，就令 $a_i=-1$.

这样就得到周期等于 p 的 L 序列的一个周期

$$a_0,\ a_1,\ a_2,\ \cdots,\ a_{p-1}.$$

再来介绍霍尔(Hall)序列. 设 p 是可以表成形状 $4x^2+27$

表 1　小于 1000 的形状 $p=4t-1$ 的素数表

t	1	2	3	5	6	8	11	12	15	17	18	20	21	26	27	32	33	35
p	3	7	11	19	23	31	43	47	59	67	71	79	83	103	107	127	131	139
t	38	41	42	45	48	50	53	56	57	60	63	66	68	71	77	78	83	87
p	151	163	167	179	191	199	211	223	227	239	251	263	271	283	307	311	331	347
t	90	92	95	96	105	108	110	111	116	117	120	122	123	125	126	131	137	141
p	359	367	379	383	419	431	439	443	463	467	479	487	491	499	503	523	547	563
t	143	147	150	152	155	158	161	162	165	171	173	180	182	185	186	188	197	203
p	571	587	599	607	619	631	643	647	659	683	691	719	727	739	743	751	787	811
t	206	207	210	215	216	221	222	227	228	230	237	242	243	246	248			
p	823	827	839	859	863	883	887	907	911	919	947	967	971	983	991			

的素数，其中 x 是个正整数. 在域 $\mathbf{Z}_p$ 中任选一个本原元 ξ，即 $\mathbf{Z}_p$ 的乘法群 $\mathbf{Z}_p^*$ 的一个生成元，特别，可以选 ξ 是 $\mathbf{Z}_p$ 的最小本原元. 定义一个序列

$$a_0,\ a_1,\ a_2,\ \cdots,$$

其中

$$a_i=\begin{cases}+1, & \text{如果 } i\equiv\xi^t(\operatorname{mod}p) \text{ 而 } t\equiv0,\ 1 \text{ 或 } 3(\operatorname{mod}6),\\ -1, & \text{其余情形}.\end{cases}$$

这样我们就得到一个周期等于 p 的二元序列，而且可以证明这是个伪随机序列. 这个序列就叫做霍尔序列.

表 2　形状 $4x^2+27$ 的素数和它的最小本原元表

x	1	2	5	7	14	16	19	20
$p=4x^2+27$	31	43	127	223	811	1051	1471	1627
最小本原元	3	3	3	3	3	7	6	3

根据霍尔序列的定义，可以写出产生霍尔序列的一个算法，这个算法是可以编成程序的.

产生霍尔(Hall)序列的算法　设 p 是形状 $4x^2+27$ 的一个素数.

(1) 在 $\mathbf{Z}_p$ 中选定一个本原元 ξ.

(2) 对于适合条件 $t\equiv0,\ 1$ 或 $3(\operatorname{mod}6)$ 的小于 $p-1$ 的非负整数 t，按大小为序计算 $(\xi^t)_p$.

(3) 依次查找 $i=0,\ 1,\ 2,\ \cdots,\ p-1$ 是否在第(2)步算出的数里出现. 如果出现，就令 $a_i=+1$；如果不出现，就令 $a_i=-1$.

这样就得到周期等于 $p=4x^2+27$ 的霍尔序列的一个周期：

$$a_0,\ a_1,\ a_2,\ \cdots,\ a_{p-1}.$$

现在利用这个算法来造一个周期等于 31 的霍尔序列.

先选定一个 mod 31 的原根 3. 再对于适合条件 $t\equiv 0, 1$ 或 $3 \pmod 6$ 的小于 $p-1$ 的非负整数 t, 计算 $(3^t)_{31}$. 将计算结果列成下表

t	0	1	3	6	7	9	12	13	15	18	19	21	24	25	27
$(3^t)_{31}$	1	3	27	16	17	29	8	24	30	4	12	15	2	6	23

根据这个表就可以写出周期等于 31 的霍尔序列

$$
\begin{array}{ccccccccccc}
-1 & +1 & +1 & +1 & +1 & & -1 & +1 & -1 & +1 & -1 \\
-1 & -1 & +1 & -1 & -1 & & +1 & +1 & +1 & -1 & -1 \\
-1 & -1 & -1 & +1 & +1 & & -1 & -1 & +1 & -1 & +1 \\
+1 & & & & & & & & & &
\end{array}
$$

我们再把 $p=43, 127$ 的霍尔序列列在表 3 里.

最后再介绍孪生素数序列. 如果 p 和 $p+2$ 都是素数, 我们就说 $(p, p+2)$ 是一对孪生素数. 定义一个序列

$$a_0, a_1, a_2, \cdots,$$

其中
$$a_i=\begin{cases}\left(\dfrac{i}{p}\right)\left(\dfrac{i}{p+2}\right), & \text{如果 } (i, p(p+2))=1, \\ +1, & \text{如果 } i\equiv 0 \pmod{p+2}, \\ -1, & \text{其余情形.}\end{cases}$$

我们就得到一个周期等于 $p(p+2)$ 的序列. 这个序列也可以证明是伪随机序列. 我们把它叫做孪生素数序列.

根据孪生素数序列的定义, 可以写出产生孪生素数序列的算法.

产生孪生素数序列的算法 设 $(p, p+2)$ 是一对孪生素数.

(1) 按产生 L 序列的算法求出周期等于 p 的 L 序列的一个周期和周期等于 $p+2$ 的 L 序列的一个周期;

表 3　霍尔序列的表

$p=43$														
−1	+1	+1	+1	+1	+1	−1	−1	+1	−1	−1	+1	+1	−1	−1
−1	+1	−1	−1	+1	+1	+1	+1	−1	−1	−1	−1	+1	−1	−1
−1	−1	+1	+1	−1	+1	−1	+1	−1	+1	−1	+1	+1		
$p=127$														
−1	+1	+1	+1	+1	+1	+1	+1	+1	−1	+1	−1	+1	−1	+1
−1	+1	−1	−1	+1	+1	−1	−1	+1	+1	+1	−1	+1	+1	−1
−1	−1	+1	+1	−1	−1	−1	−1	+1	−1	+1	−1	−1	−1	−1
−1	+1	+1	+1	−1	+1	+1	−1	−1	+1	−1	+1	+1	−1	−1
−1	+1	−1	+1	+1	+1	+1	+1	−1	−1	−1	−1	−1	+1	−1
+1	+1	+1	−1	−1	+1	−1	−1	−1	−1	−1	−1	+1	−1	+1
−1	−1	+1	−1	+1	+1	+1	+1	−1	−1	+1	+1	+1	−1	−1
−1	−1	+1	+1	−1	−1	+1	+1	−1	+1	−1	−1	+1	−1	+1
−1	−1	+1	+1	−1	+1	+1								

$$\left(\frac{0}{p}\right),\ \left(\frac{1}{p}\right),\ \left(\frac{2}{p}\right),\ \cdots,\ \left(\frac{p-1}{p}\right).$$

$$\left(\frac{0}{p+2}\right),\ \left(\frac{1}{p+2}\right),\ \left(\frac{2}{p+2}\right),\ \cdots,\ \left(\frac{p+1}{p+2}\right).$$

(2) 对于 $i=0,\ 1,\ 2,\ \cdots,\ p(p+2)-1$，如果 $(i,\ p(p+2))=1$，就令

$$a_i=\left(\frac{i}{p}\right)\left(\frac{i}{p+2}\right);$$

如果 $i\equiv 0(\bmod p+2)$，就令

$$a_i=+1;$$

如果 $i\equiv 0(\bmod p)$ 而 $i\not\equiv 0(\bmod p+2)$，就令

$$a_i=-1.$$

这样就得到周期等于 $p(p+2)$ 的孪生素数序列的一个周期

$$a_0,\ a_1,\ a_2,\ \cdots,\ a_{p(p+2)-1}.$$

现在我们利用这个算法来求周期等于 $15=3\times 5$ 的孪生素数序列．先求出

$$\left(\frac{0}{3}\right)=+1,\ \left(\frac{1}{3}\right)=+1,\ \left(\frac{2}{3}\right)=-1,$$
$$\left(\frac{0}{5}\right)=+1,\ \left(\frac{1}{5}\right)=+1,\ \left(\frac{2}{5}\right)=-1,$$
$$\left(\frac{3}{5}\right)=-1,\ \left(\frac{4}{5}\right)=+1.$$

再依序计算

$$a_0=+1, \qquad a_1=\left(\frac{1}{3}\right)\left(\frac{1}{5}\right)=+1,$$
$$a_2=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=+1, \qquad a_3=-1,$$
$$a_4=\left(\frac{4}{3}\right)\left(\frac{4}{5}\right)=\left(\frac{1}{3}\right)\left(\frac{4}{5}\right)=+1,$$
$$a_5=+1, \qquad a_6=-1,$$
$$a_7=\left(\frac{7}{3}\right)\left(\frac{7}{5}\right)=\left(\frac{1}{3}\right)\left(\frac{2}{5}\right)=-1,$$
$$a_8=\left(\frac{8}{3}\right)\left(\frac{8}{5}\right)=+1, \qquad a_9=-1,$$
$$a_{10}=+1, \qquad a_{11}=\left(\frac{11}{3}\right)\left(\frac{11}{5}\right)=-1,$$
$$a_{12}=-1, \qquad a_{13}=\left(\frac{13}{3}\right)\left(\frac{13}{5}\right)=-1,$$
$$a_{14}=\left(\frac{14}{3}\right)\left(\frac{14}{5}\right)=-1.$$

这样我们就得到周期等于 15 的孪生素数序列的一个周期:

+1 +1 +1 −1 +1 +1 −1 −1 +1 −1
+1 −1 −1 −1 −1

同样可以求出周期等于 $35=5\cdot7$ 的孪生素数序列的一个周期

+1 +1 −1 +1 +1 −1 −1 +1 −1 +1
−1 +1 +1 +1 +1 −1 +1 +1 −1 −1

$-1\ \ +1\ \ -1\ \ -1\ \ -1\qquad -1\ \ -1\ \ +1\ \ +1\ \ +1$

$-1\ \ -1\ \ -1\ \ +1\ \ -1$

至于怎样用硬件产生 L 序列，霍尔序列以及孪生素数序列的问题将在下两节中介绍.

§8 线性移位寄存器的综合

在这一节里，仍设 $\mathbf{F}_q$ 是 q 个元素的有限域，而 q 是一个素数的幂. 一般我们并不假定 $q=2$.

设 N 是一个正整数，而

$$a_0,\ a_1,\ a_2,\ \cdots,\ a_{N-1}\quad (a_i\in\mathbf{F}_q,\ 0\leqslant i\leqslant N-1)\tag{1}$$

是 $\mathbf{F}_q$ 上的一个有限序列，它的项数 N 叫做这个序列的长. 我们也把 (1) 叫做一个长为 N 的 q 元序列. 再设

$$f(x)=1+c_1x+c_2x^2+\cdots+c_lx^l\tag{2}$$

是 $\mathbf{F}_q$ 上的一个多项式，而 $l\geqslant 1$. 我们把以 $f(x)$ 为联接多项式的 l 级线性移位寄存器

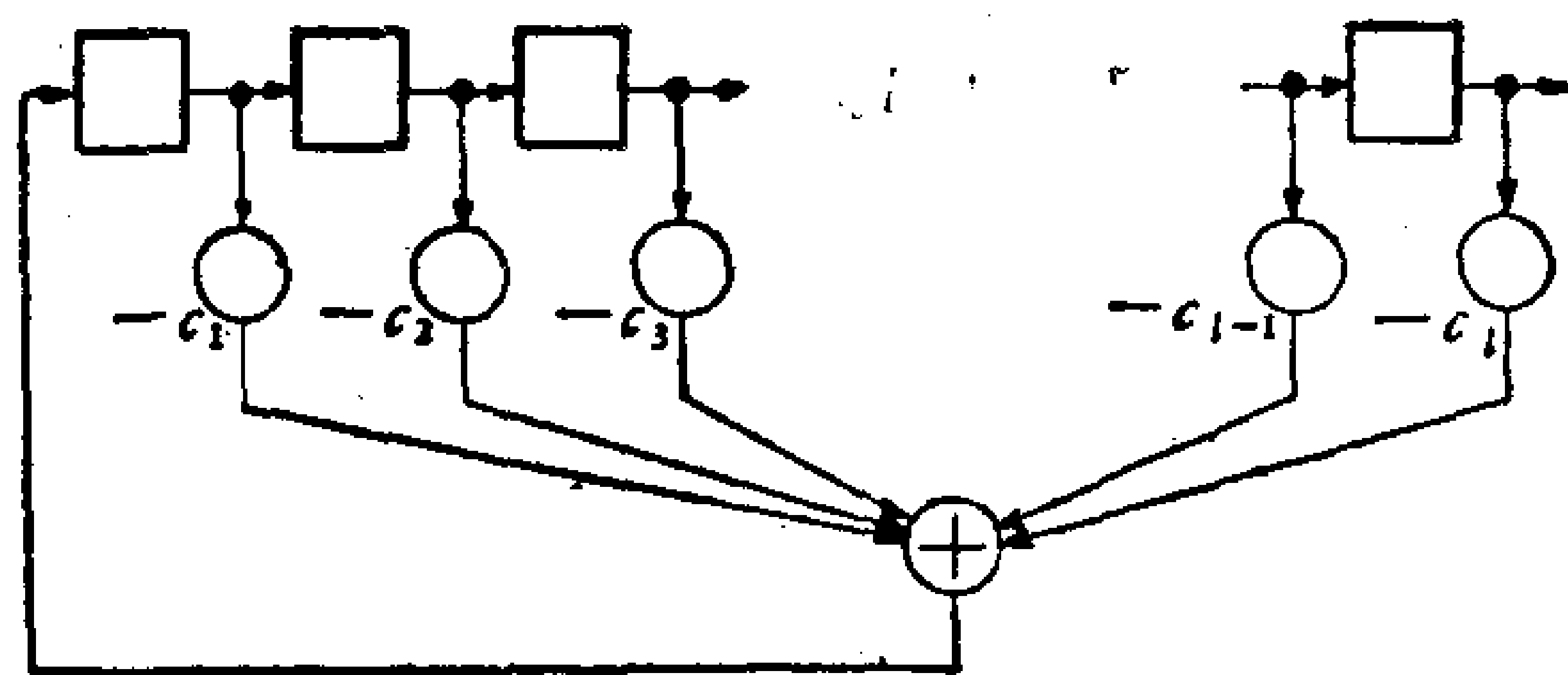


图 1

简记作 $\langle f(x),\ l\rangle$. 注意，我们并不假定 $c_l\neq 0$，即 $\langle f(x),\ l\rangle$ 可以是退化的. 我们说 $\langle f(x),\ l\rangle$ 从初始状态 $(a_0,\ a_1,\ \cdots,\ a_{l-1})$ 出发产生(1)，简称 $\langle f(x),\ l\rangle$ 产生(1)，如果

$$a_k=-(c_1a_{k-1}+c_2a_{k-2}+\cdots+c_la_{k-l}),\quad k=l,\ l+1,\ \cdots,\ N-1.\tag{3}$$

所谓线性移位寄存器的综合问题就是：给定一个长为 N 的 q 元序列(1)，去求出产生它的线性移位寄存器. 显然，当 $l \geqslant N$ 时，任一 l 级线性移位寄存器都可以产生(1). 因此如果对产生(1)的线性移位寄存器的级数不加限制，那么线性移位寄存器的综合问题很容易求解，而且有无穷多组解. 所以线性移位寄存器的综合问题应该这样提出：

"任给一个长为 N 的 q 元序列 (1)，如何去求出产生 (1) 的一个级数最小的线性移位寄存器，即最短的线性移位寄存器？更进一步，产生(1)的最短线性移位寄存器是否唯一？什么时候唯一？如果不唯一，怎样把它们都求出来？"

在讨论这个综合问题之前，我们先给出线性移位寄存器 $\langle f(x), l\rangle$ 产生长为 N 的 q 元序列 (1) 的一个必要充分条件.

引理 1 设有一个长为 N 的 q 元序列(1)，而 $f(x)$ 如(2). 令

$$a(x)=a_0+a_1x+a_2x^2+\cdots+a_{N-1}x^{N-1},$$

并将 $f(x)a(x)$ 中 k 次项的系数记作 $[f(x)a(x)]_k$，那么 $\langle f(x), l\rangle$ 产生(1)，当且仅当

$$[f(x)a(x)]_k=0, k=l, l+1, \cdots, N-1.$$

证. 我们有

$$[f(x)a(x)]_k=a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_la_{k-l},$$
$$k=l, l+1, \cdots, N-1.$$

因此本引理成立.

我们约定，所谓的 0 级线性移位寄存器是以 $f(x)=1$ 为联接多项式的线性移位寄存器；并约定，长为 N 的零序列

$$\underbrace{0, 0, \cdots, 0}_{N\text{个}0}$$

由 0 级线性移位寄存器产生，而且 0 级线性移位寄存器只能产生零序列. 这个约定是合理的，因为

$$[1\cdot(0+0\cdot x+0\cdot x^2+\cdots+0\cdot x^{N-1})]_k=0,$$
$$k=0,\ 1,\ 2,\ \cdots,\ N-1.$$

这是和引理1相符的.

下面我们要介绍解前述线性移位寄存器综合问题的一个迭代算法. 这个算法是梅西 (J. L. Massey) 建议的*. 他并指出这个算法实质上就是 E. R. Berlekamp 建议的, 译 BCH 码时, 从校验子求找错位多项式的算法**. 但梅西 (Massey) 的算法化简了 Berlekamp 原来的算法. 这个算法是用数学归纳法去求一系列的线性移位寄存器

$$\langle f_n(x),\ l_n\rangle,\ n=1,\ 2,\ \cdots,\ N$$

(自然要求 $\partial^0 f_n(x)\leqslant l_n$), 而每一个 $\langle f_n(x),\ l_n\rangle$ 都是产生(1)的前 n 项的一个最短的线性移位寄存器. 根据引理1, 这就是说, 对每一个 $n=1,\ 2,\ \cdots,\ N$, 求一个多项式 $f_n(x)$ 和一个 $\geqslant\partial^0 f_n(x)$ 的整数 l_n, 使

$$[f_n(x)a(x)]_k=0,\ k=l_n,\ l_n+1,\ \cdots,\ n-1, \tag{4}$$

并且 l_n 是最小的非负整数使得有次数 $\leqslant l_n$ 的多项式 $f_n(x)$ 满足条件(4).

解线性移位寄存器综合问题的一个迭代算法 任给一个长为 N 的 q 元序列 (1). 对 n 用数学归纳法来定义一系列的

$$\langle f_n(x),\ l_n\rangle,n=1,\ 2,\ \cdots,\ N.$$

(1) 设 n_0 是个非负整数使

$$a_0=a_1=a_2=\cdots=a_{n_0-1}=0,\ a_{n_0}\neq 0,$$

那么约定 $\quad d_0=d_1=d_2=\cdots=d_{n_0-1}=0,\ d_{n_0}=a_{n_0},$

并令 $\quad f_1(x)=f_2(x)=\cdots=f_{n_0}(x)=1,$

$$l_1=l_2=\cdots=l_{n_0}=0,$$

---

* 见 Massey, J. L., Shift-Register Synthesis and BCH Decoding, IEEE Trans. on Information Theory, **15**(1969), 122—127.

** 见 [17], 第七章

同时可以取任意一个n_0+1级线性移位寄存器作为$\langle f_{n_0+1}(x), l_{n_0+1}\rangle$，但为了确定起见，令

$$f_{n_0+1}(x)=1-d_{n_0}x^{n_0+1},\ l_{n_0+1}=n_0+1.$$

(2) 设$\langle f_i(x), l_i\rangle$, $i=1, 2, \cdots, n(n_0<n<N)$已求得，而

$$l_1=l_2=\cdots=l_{n_0}<l_{n_0+1}\leqslant l_{n_0+2}\leqslant\cdots\leqslant l_n.$$

令 $$f_n(x)=1+c_{n1}x+c_{n2}x^2+\cdots+c_{nl_n}x^{l_n},$$

计算 $$d_n=a_n+c_{n1}a_{n-1}+c_{n2}a_{n-2}+\cdots+c_{nl_n}a_{n-l_n}.$$

区别下面两个情形：

2.1) $d_n=0$. 这时令

$$f_{n+1}(x)=f_n(x),\ l_{n+1}=l_n.$$

2.2) $d_n\neq0$. 这时有$m(1\leqslant m<n)$使

$$l_m<l_{m+1}=l_{m+2}=\cdots=l_n,$$

那么令 $$f_{n+1}(x)=f_n(x)-d_nd_m^{-1}x^{n-m}f_m(x),$$

$$l_{n+1}=\max\{l_n,\ n+1-l_n\}.$$

最后我们得到产生(1)的一个最短线性移位寄存器

$$\langle f_N(x),\ l_N\rangle.$$

今后我们把这个算法简称为综合算法.

下面我们要证明，按综合算法求出的$\langle f_N(x), l_N\rangle$确实是产生(1)的最短线性移位寄存器. 但我们先举几个例子来帮助读者熟悉这个算法.

例1 求产生周期等于11的二次剩余序列的一个周期的最短线性移位寄存器.

周期等于11的二次剩余序列的一个周期是

+1 +1 −1 +1 +1 +1 −1 −1 −1 +1 −1

(参看上一节中二次剩余序列部分). 将它变成0, 1序列:

0 0 1 0 0 0 1 1 1 0 1,

那么 $a_0=0,\ a_1=0,\ a_2=1,\ a_3=0,\ a_4=0,\ a_5=0,$

$$a_6=1,\ a_7=1,\ a_8=1,\ a_9=0,\ a_{10}=1.$$

按综合算法去求产生它的最短线性移位寄存器:

第 1 步 $d_0=a_0=0$, 那么

$f_1(x)=1,\ l_1=0.$

第 2 步 $d_1=a_1=0$, 那么

$f_2(x)=f_1(x)=1,\ l_2=l_1=0.$

第 3 步 $d_2=a_2=1$, 那么

$f_3(x)=1+x^3,\ l_3=3.$

第 4 步 计算 $d_3=a_3+a_0=0$, 那么

$f_4(x)=f_3(x)=1+x^3,\ l_4=l_3=3.$

第 5 步 计算 $d_4=a_4+a_1=0$, 那么

$f_5(x)=f_4(x)=1+x^3,\ l_5=l_4=3.$

第 6 步 计算 $d_5=a_5+a_2=1$, 那么

$f_6(x)=f_5(x)+x^{5-2}f_2(x)=1,$

$l_6=\max\{l_5,\ 5+1-l_5\}=3.$

第 7 步 计算 $d_6=a_6=1$, 那么

$f_7(x)=f_6(x)+x^{6-2}f_2(x)=1+x^4,$

$l_7=\max\{l_6,\ 6+1-l_6\}=4.$

第 8 步 计算 $d_7=a_7+a_3=1$, 那么

$f_8(x)=f_7(x)+x^{7-6}f_6(x)=1+x+x^4,$

$l_8=\max\{l_7,\ 7+1-l_7\}=4.$

第 9 步 计算 $d_8=a_8+a_7+a_4=0$, 那么

$f_9(x)=f_8(x)=1+x+x^4,\ l_9=l_8=4$

第 10 步 计算 $d_9=a_9+a_8+a_5=1$, 那么

$f_{10}=f_9(x)+x^{9-6}f_6(x)=1+x+x^3+x^4,$

$l_{10}=\max\{l_9,\ 9+1-l_9\}=6$

第 11 步 计算 $d_{10}=a_{10}+a_9+a_7+a_6=1$, 那么

$f_{11}=f_{10}(x)+x^{10-9}f_9(x)=1+x^2+x^3+x^4+x^5,$

$$l_{11}=\max\{l_{10},\ 10+1-l_{10}\}=6.$$

因此，$\langle 1+x^2+x^3+x^4+x^5,\ 6\rangle$ 就是产生周期等于 11 的二次剩余序列的一个周期的最短线性移位寄存器.

可以把上面的计算过程列成一个表

表 1

步数 (n)	d_{n-1}	$f_n(x)$	l_n
1	0	1	0
2	0	1	0
3	1	$1+x^3$	3
4	0	$1+x^3$	3
5	0	$1+x^3$	3
6	1	1	3
7	1	$1+x^4$	4
8	1	$1+x+x^4$	4
9	0	$1+x+x^4$	4
10	1	$1+x+x^3+x^4$	6
11	1	$1+x^2+x^3+x^4+x^5$	6

例 2 求产生周期 15 的二元 m 序列的一个周期

$$0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1$$

的最短线性移位寄存器.

将按综合算法的计算过程列成表 2.

于是 $\langle 1+x^3+x^4,\ 4\rangle$ 是产生周期等于 15 的二元 m 序列的一个周期的最短线性移位寄存器.

为了证明按综合算法求出的 $\langle f_N(x),\ l_N\rangle$ 确是产生(1)的最短线性移位寄存器，我们先来证明下面这两条引理.

引理 2 设有一个长为 $n+1$ 的 q 元序列

$$a_0,\ a_1,\ a_2,\ \cdots,\ a_n. \tag{5}$$

并假定有一个 $\langle f(x),\ l\rangle$ 能产生(5)的前 n 项，而不能产生

表 2

步数 (n)	d_{n-1}	$f_n(x)$	l_n
1	0	1	0
2	0	1	0
3	0	1	0
4	1	$1+x^4$	4
5	0	$1+x^4$	4
6	0	$1+x^4$	4
7	1	$1+x^3+x^4$	4
8	0	$1+x^3+x^4$	4
9	0	$1+x^3+x^4$	4
10	0	$1+x^3+x^4$	4
11	0	$1+x^3+x^4$	4
12	0	$1+x^3+x^4$	4
13	0	$1+x^3+x^4$	4
14	0	$1+x^3+x^4$	4
15	0	$1+x^3+x^4$	4

(5)，那么任何一个能产生 (5) 的线性移位寄存器的级数 l' 必适合条件

$$l' \geqslant n+1-l.$$

证．当 $l>n$ 时，因任一 l 级线性移位寄存器都能产生 (5)，所以这时本引理的前提不成立．

当 $l=n$ 时，本引理的结论是要求 $l' \geqslant 1$．如果 $l'=0$，(5) 就必须是零序列，这时 $\langle f(x), l\rangle$ 从全 0 状态出发就能产生 (5)，因此这时本引理的前提也不成立．如果 $l'>0$，那么 $l' \geqslant 1$ 自然成立．

从下设 $l<n$，并假定 $\langle f_1(x), l'\rangle$ 能产生(5)，设

$$f(x)=1+c_1x+c_2x^2+\cdots+c_lx^l,$$
$$f_1(x)=1+c_1'x+c_2'x^2+\cdots+c_{l'}'x^{l'},$$

那么

$$-\sum_{i=1}^{l} c_i a_{k-i} \begin{cases} = a_k, & \text{如 } k = l,\ l+1,\ \cdots,\ n-1, \\ \neq a_n, & \text{如 } k = n, \end{cases} \tag{6}$$

$$-\sum_{i=1}^{l'} c'_i a_{k-i} = a_k, \quad \text{如 } k = l',\ l'+1,\ \cdots,\ n-1,\ n. \tag{7}$$

如果本引理不成立，那么 $l' \leqslant n-l$，这时 $\{a_{n-l}, a_{n-l+1}, \cdots, a_{n-1}\}$ 就是 $\{a_{l'}, a_{l'+1}, \cdots, a_{n-1}, a_n\}$ 的子集. 于是利用(7)式，有

$$\begin{aligned} -\sum_{i=1}^{l} c_i a_{n-i} &= \sum_{i=1}^{l} c_i \sum_{j=1}^{l'} c'_j a_{n-i-j} \\ &= \sum_{j=1}^{l'} c'_j \sum_{i=1}^{l} c_i a_{n-i-j}. \end{aligned}$$

从 $l' \leqslant n-l$ 推出 $l \leqslant n-l'$，因此 $\{a_{n-l'}, a_{n-l'+1}, \cdots, a_{n-1}\}$ 是 $\{a_l, a_{l+1}, \cdots, a_{n-1}\}$ 的子集. 那么利用(6)式可以将上式右侧写成

$$\sum_{j=1}^{l'} c'_j \sum_{i=1}^{l} c_i a_{n-i-j} = -\sum_{j=1}^{l'} c'_j a_{n-j}.$$

再根据(7)式，

$$-\sum_{j=1}^{l'} c'_j a_{n-j} = a_n.$$

因此有

$$-\sum_{i=1}^{l} c_i a_{n-i} = a_n.$$

这就是说，$\langle f(x), l\rangle$ 产生(5)，这和本引理的假设相矛盾. 因此 $l' \leqslant n-l$ 这一假定不能成立. 所以一定有 $l' \geqslant n+1-l$.

引理 3 设(1)是一个长为 N 的 q 元序列. 用 l_n 表示产生(1)的前 n 项的最短线性移位寄存器的级数 $(n=1, 2, \cdots, N)$. 那么 l_n 是 n 的一个单调不减函数(即如果 $n \leqslant m$，则 $l_n \leqslant l_m$)，而 $l_n \leqslant N$. 更进一步，如果某个 l_n 级的线性移位寄存器产生(1)的前 n 项，而不能产生(1)的前 $n+1$ 项，那么

$$l_{n+1} \geqslant \max\{l_n,\ n+1-l_n\}. \tag{8}$$

证. l_n 是 n 的单调不减函数及 $l_n \leqslant N$ 都是很显然的. 现

在去证明本引理中后面的一个断言．由 l_n 的单调不减性，有

$$l_{n+1} \geqslant l_n.$$

如果有某个 l_n 级的线性移位寄存器产生(1)的前 n 项，而不能产生(1)的前 $n+1$ 项，那么根据引理2有

$$l_{n+1} \geqslant n+1-l_n.$$

由上面这两个不等式就可以推出(8)．

现在我们来证明

定理1 任给一个长为 N 的 q 元序列(1)，那么按综合算法求出的每一个 $\langle f_n(x), l_n \rangle (n=1, 2, \cdots, N)$ 确是产生(1)的前 n 项的一个最短线性移位寄存器．更进一步，对 $n=1, 2, \cdots, N-2$，如果 $\langle f_n(x), l_n \rangle$ 产生(1)的前 $n+1$ 项，那么 $l_{n+1}=l_n$；如果 $\langle f_n(x), l_n \rangle$ 不能产生(1)的前 $n+1$ 项，那么 $l_{n+1}=\max\{l_n, n+1-l_n\}$．

证．我们对 n 用数学归纳法来证明．

设 n_0 是最小非负整数使

$$a_0=a_1=a_2=\cdots=a_{n_0-1}=0, \quad a_{n_0} \neq 0.$$

根据综合算法，

$$f_1(x)=f_2(x)=\cdots=f_{n_0}(x)=1,$$
$$l_1=l_2=\cdots=l_{n_0}=0.$$

按照我们的约定，0级线性移位寄存器产生(1)的前 $n \leqslant n_0$ 项，而且当然是产生(1)的前 $n \leqslant n_0$ 项的最短线性移位寄存器．因此本定理的第一个断言对于 $n \leqslant n_0$ 成立，而第二个断言对于 $n \leqslant n_0-1$ 成立．

仍根据综合算法，

$$f_{n_0+1}(x)=1-d_{n_0}x^{n_0+1}, \quad l_{n_0+1}=n_0+1.$$

显然，n_0+1 级线性移位寄存器 $\langle f_{n_0+1}(x), l_{n_0+1} \rangle$ 产生(1)的前 n_0+1 项，而且级数 $<n_0+1$ 的任一线性移位寄存器都不能产生(1)的前 n_0+1 项，所以本定理的第一个断言对于

$n=n_0+1$ 成立. 这时 $l_{n_0}=0$, 因此

$$\max\{l_{n_0},\ n_0+1-l_{n_0}\}=\max\{0,\ n_0+1\}=n_0+1=l_{n_0+1}.$$

所以本定理的第二个断言对于 $n=n_0$ 成立.

现在设 $n_0\leqslant n<N$, 并假定本定理对于 1, 2, …, n 都成立, 我们去证明它对于 $n+1$ 也成立. 首先, 根据引理 3, 或直接从

$$l_{i+1}=l_i \text{ 或 } \max\{l_i,\ i+1-l_i\},\ i=1,\ 2,\ \cdots,\ n-1$$

导出

$$l_1\leqslant l_2\leqslant\cdots\leqslant l_n.$$

根据综合算法,

$$d_n=a_n+c_{n1}a_{n-1}+c_{n2}a_{n-2}+\cdots+c_{nl_n}a_{n-l_n}.$$

如果 $d_n=0$, 那么根据综合算法,

$$f_{n+1}(x)=f_n(x),\ \ l_{n+1}=l_n.$$

根据归纳法假设, $\langle f_n(x),\ l_n\rangle$ 是产生(1)的前 n 项的一个最短线性移位寄存器. 又因为 $d_n=0$, 所以 $\langle f_n(x),\ l_n\rangle$ 也能产生(1)的前 $n+1$ 项, 因此 $\langle f_{n+1}(x),\ l_{n+1}\rangle=\langle f_n(x),\ l_n\rangle$ 是产生(1)的前 $n+1$ 项的一个最短线性移位寄存器. 这时有 $l^{n+1}=l_n$.

如果 $d_n\neq 0$, 那么有 $m(1\leqslant m<n)$ 使

$$l_m<l_{m+1}=l_{m+2}=\cdots=l_n.$$

因 $l_m<l_{m+1}$, 根据归纳法假设一定有 $d_m\neq 0$. 仍根据综合算法,

$$f_{n+1}(x)=f_n(x)-d_nd_m^{-1}x^{n-m}f_m(x),$$

$$l_{n+1}=\max\{l_n,\ n+1-l_n\},$$

我们有

$$\partial^0 f_{n+1}(x)\leqslant\max\{\partial^0 f_n(x),\ n-m+\partial^0 f_m(x)\}$$

$$\leqslant\max\{l_n,\ n-m+l_m\},$$

根据归纳法假设

$$l_{m+1}=\max\{l_m,\ m+1-l_m\}.$$

但是 $l_m<l_{m+1}=l_n$, 所以

$$l_n = l_{m+1} = m+1-l_m.$$

因此

$$\partial^0 f_{n+1}(x) \leqslant \max\{l_n,\ n+1-l_n\} = l_{n+1}.$$

这证明了 $\langle f_{n+1}(x),\ l_{n+1}\rangle$ 是个 l_{n+1} 级线性移位寄存器. 又因 $\langle f_n(x),\ l_n\rangle$ 产生(1)的前 n 项, 而 $\langle f_m(x),\ l_m\rangle$ 产生(1)的前 m 项, 我们有

$$\begin{aligned} a_k + \sum_{i=1}^{l_{n+1}} c_{n+1\,i} a_{k-i} &= a_k + \sum_{i=1}^{l_n} c_{ni} a_{k-i} \\ &\quad - d_n d_m^{-1} \left(a_{k-n+m} + \sum_{i=1}^{l_m} c_{mi} a_{k-n+m-i} \right) \\ &= \begin{cases} 0, & \text{如 } k = l_{n+1},\ l_{n+1}+1,\ \cdots,\ n-1, \\ d_n - d_n d_m^{-1} d_m = 0, & \text{如 } k = n. \end{cases} \end{aligned}$$

这证明了 $\langle f_{n+1}(x),\ l_{n+1}\rangle$ 产生 (1) 的前 $n+1$ 项. 因 $d_n \neq 0$, $\langle f_n(x),\ l_n\rangle$ 不能产生(1)的前 $n+1$ 项, 所以根据引理 3, 产生(1)的前 $n+1$ 项的线性移位寄存器的级数的极小值一定 $\geqslant \max\{l_n,\ n+1-l_n\}$. 今 $l_{n+1} = \max\{l_n,\ n+1-l_n\}$, 所以 $\langle f_{n+1}(x),\ l_{n+1}\rangle$ 是产生(1)的前 $n+1$ 项的一个最短线性移位寄存器.

这证明了定理 1 对 $n+1$ 也成立.

根据数学归纳法可知定理 1 成立.

特别, 根据定理 1 可知, 综合算法提供了求产生任一给定的 q 元周期序列(当然也包括二元伪随机序列)的一个周期的一个最短线性移位寄存器的一个算法. 下面我们还要指出, 综合算法还提供了求产生任一给定的 q 元周期序列(而不只是它的一个周期)的一个最短线性移位寄存器的一个算法.

我们先来讨论产生 (1) 的最短线性移位寄存器的唯一性问题. 先证明一条引理.

引理 4 任给一个长为 N 的 q 元序列 (1). 对 $n=1,\ 2,\ \cdots,\ N$, 用 l_n 表示产生(1)的前 n 项的最短线性移位寄存器

的级数. 如果 $l_{n+1}>l_n$, 那么 $2l_n\leqslant n$ 而且任一产生(1)的前 n 项的 l_n 级线性移位寄存器都不能产生(1)的前 $n+1$ 项. 反过来, 如果 $2l_n\leqslant n$ 而且某个产生(1)的前 n 项的 l_n 级线性移位寄存器不能产生(1)的前 $n+1$ 项, 那么 $l_{n+1}>l_n$.

证. 先设 $l_{n+1}>l_n$. 那么显然任一产生(1)的前 n 项的 l_n 级线性移位寄存器都不能产生(1)的前 $n+1$ 项. 特别, 按综合算法求得的 $\langle f_n(x), l_n\rangle$ 不能产生(1)的前 $n+1$ 项. 于是根据定理1就有

$$l_{n+1}=\max\{l_n, n+1-l_n\}.$$

考虑到 $l_{n+1}>l_n$, 所以一定有 $n+1-l_n>l_n$. 因此 $2l_n\leqslant n$.

反过来, 设 $2l_n\leqslant n$, 并设某个产生(1)的前 n 项的 l_n 级线性移位寄存器不能产生(1)的前 $n+1$ 项, 那么根据引理3就有

$$l_{n+1}\geqslant\max\{l_n, n+1-l_n\}.$$

从 $2l_n\leqslant n$ 推出 $n+1-l_n>l_n$. 因此

$$l_{n+1}\geqslant\max\{l_n, n+1-l_n\}=n+1-l_n>l_n.$$

定理 2 任给一个长为 N 的 q 元序列(1), 并假定产生(1)的最短线性移位寄存器的级数是 l_N, 那么产生(1)的最短线性移位寄存器是唯一的, 当且仅当 $2l_N\leqslant N$.

证. 先假定 $2l_N>N$. 设 $\langle f_N(x), l_N\rangle$ 是按综合算法造出的产生(1)的最短线性移位寄存器. 写

$$f_N(x)=1+c_1x+c_2x^2+\cdots+c_{l_N}x^{l_N},$$

那么

$$a_k=-\sum_{i=1}^{l_N}c_ia_{k-i}, k=l_N, l_N+1, \cdots, N-1.$$

任选 $a_N\in\mathbf{F}_q$ 使

$$a_N\neq-\sum_{i=1}^{l_N}c_ia_{N-i},$$

那么 $\langle f_N(x), l_N\rangle$ 不能产生长为 $N+1$ 的 q 元序列

$$a_0, a_1, a_2, \cdots, a_{N-1}, a_N. \tag{9}$$

于是根据综合算法造出的产生(9)的 $\langle f_{N+1}(x), l_{N+1}\rangle$ 就不是 $\langle f_N(x), l_N\rangle$. 但 $2l_N>N$, 根据引理 4, 我们有 $l_{N+1}=l_N$. 因此 $\langle f_{N+1}(x), l_{N+1}\rangle$ 也是产生(1)的一个 $l_{N+1}=l_N$ 级线性移位寄存器. 于是产生(1)的最短线性移位寄存器不唯一.

再假定 $2l_N\leqslant N$. 我们要证明, 这时产生(1)的最短线性移位寄存器是唯一的. 设 $\langle f(x), l_N\rangle$ 和 $\langle f_1(x), l_N\rangle$ 都是产生(1)的最短线性移位寄存器. 我们要证明 $f(x)=f_1(x)$. 写

$$f(x)=1+c_1x+c_2x^2+\cdots+c_{l_N}x^{l_N},$$
$$f_1(x)=1+c_1'x+c_2'x^2+\cdots+c_{l_N}'x^{l_N}.$$

那么
$$\begin{aligned}a_k&=-(c_1a_{k-1}+c_2a_{k-2}+\cdots+c_{l_N}a_{k-l_N})\\&=-(c_1'a_{k-1}+c_2'a_{k-2}+\cdots+c_{l_N}'a_{k-l_N}),\\&\qquad k=l_N, l_N+1, \cdots, N-1.\end{aligned}$$

归纳地定义
$$a_k=-(c_1a_{k-1}+c_2a_{k-2}+\cdots+c_{l_N}a_{k-l_N}),\quad k=N, N+1, \cdots,$$

那么 $\langle f(x), l_N\rangle$ 也产生无限 q 元序列

$$a_0, a_1, a_2, \cdots, \tag{10}$$

而且对任意整数 $n\geqslant N$, $\langle f(x), l_N\rangle$ 也是产生(10)的前 n 项的一个最短线性移位寄存器. 因此, 如果用 l_n 表示产生(10)的前 n 项的最短线性移位寄存器的级数, 那么

$$l_n=l_{n+1}=l_{n+2}=\cdots. \tag{11}$$

我们先去证明 $\langle f_1(x), l_N\rangle$ 也产生(10). 用反证法去证明这一点. 假定 $\langle f_1(x), l_N\rangle$ 不能产生(10), 设 N' 是最小正整数使 $\langle f_1(x), l_N\rangle$ 能产生(10)的前 N' 项, 而不能产生(10)的前 $N'+1$ 项. 那么显然有 $N'\geqslant N$. 于是从 $2l_N\leqslant N$ 推出 $2l_{N'}=2l_N\leqslant N\leqslant N'$. 既然 $2l_{N'}\leqslant N'$, 而 $\langle f_1(x), l_N\rangle$ 是能产生(10)的前 N' 项, 却不能产生 (10) 的前 $N'+1$ 项的 $l_{N'}=l_N$ 级线性移位寄存器, 所以根据引理 4 就一定有 $l_{N'+1}>l_{N'}$. 这与

(11)相矛盾. 因此 $\langle f_1(x), l_N\rangle$ 一定也产生(10).

我们再去证明 $f(x)=f_1(x)$. 仍然用反证法. 假定 $f(x)\neq f_1(x)$. 那么可设 m 是最小正整数使 $c_m\neq c'_m$, 即

$$c_1=c'_1,\ c_2=c'_2,\ \cdots,\ c_{m-1}=c'_{m-1} \text{ 而 } c_m\neq c'_m. \tag{12}$$

自然有 $1\leqslant m\leqslant l_N$. 因为 $\langle f(x), l_N\rangle$ 和 $\langle f_1(x), l_N\rangle$ 都产生(10), 所以

$$a_k=-(c_1a_{k-1}+c_2a_{k-2}+\cdots+c_{l_N}a_{k-l_N}),$$
$$a_k=-(c'_1a_{k-1}+c'_2a_{k-2}+\cdots+c'_{l_N}a_{k-l_N}),$$
$$k=l_N,\ l_N+1,\ \cdots.$$

将以上二式相减, 注意到(12), 得

$$(c_m-c'_m)a_{k-m}+(c_{m+1}-c'_{m+1})a_{k-m-1}+\cdots$$
$$+(c_{l_N}-c'_{l_N})a_{k-l_N}=0,\ k=l_N,\ l_N+1,\ \cdots. \tag{13}$$

令 $\lambda_i=(c_m-c'_m)^{-1}(c_{m+i}-c'_{m+i}),\ i=1,\ 2,\ \cdots,\ l_N-m,$

那么可将(13)式改写成

$$a_{k-m}=-(\lambda_1a_{k-m-1}+\lambda_2a_{k-m-2}+\cdots$$
$$+\lambda_{l_N-m}a_{k-l_N}=0,\ k=l_N,\ l_N+1,\ \cdots. \tag{14}$$

改动(14)式足码, 可将(14)式改写成

$$a_k=-(\lambda_1a_{k-1}+\lambda_2a_{k-2}+\cdots+\lambda_{l_N-m}a_{k-l_N+m}),$$
$$k=l_N-m,\ l_N-m+1\cdots. \tag{15}$$

令 $$g(x)=1+\lambda_1x+\lambda_2x^2+\cdots+\lambda_{l_N-m}x^{l_N-m},$$

那么(15)式是说 $\langle g(x), l_N-m\rangle$ 也产生(10). 特别, $\langle g(x), l_N-m\rangle$ 产生(10)的前 N 项, 即产生(1). 但 $\langle f(x), l_N\rangle$ 是产生(1)的一个最短线性移位寄存器, 而 $l_N-m<l_N$. 这是一个矛盾. 因此 $f(x)\neq f_1(x)$ 这一假设不成立. 所以一定有 $f(x)=f_1(x)$. 这证明了, 在 $2l_N\leqslant N$ 的前提下, 产生(1)的最短线性移位寄存器是唯一的.

这样定理 2 就完全证明了.

定理 2 有下面这些有用的系理.

系理 1　任给一个长为 N 的 q 元序列(1)，并设产生(1)的最短线性移位寄存器的级数是 l_N. 假定 $2l_N \leqslant N$. 那么按综合算法算出的 $\langle f_{2l_N}(x), l_{2l_N}\rangle$ 就是产生(1)的唯一的那个最短线性移位寄存器.

证. 因为 $2l_N \leqslant N$, 所以根据定理 2, 产生(1)的最短线性移位寄存器是唯一的. 那么按综合算法算出的 $\langle f_N(x), l_N\rangle$ 就是产生(1)的唯一的那个最短线性移位寄存器. $\langle f_N(x), l_N\rangle$ 自然也产生(1)的前 $2l_N$ 项. 从 $2l_N \leqslant N$ 推出 $l_{2l_N} \leqslant l_N$, 于是 $2l_{2l_N} \leqslant 2l_N$. 那么仍根据定理 2, 产生(1)的前 $2l_N$ 项的最短线性移位寄存器是唯一的. 特别, 按综合算法算出的 $\langle f_{2l_N}(x), l_{2l_N}\rangle$ 就是产生(1)的前 $2l_N$ 项的最短线性移位寄存器.

我们去证明 $\langle f_{2l_N}(x), l_{2l_N}\rangle$ 能产生(1). 用反证法去证明这一点. 设 $\langle f_{2l_N}(x), l_{2l_N}\rangle$ 不能产生(1)，那么就有一个正整数 N' 使 $\langle f_{2l_N}(x), l_{2l_N}\rangle$ 能产生(1)的前 N' 项. 但不能产生(1)的前 $N'+1$ 项, 而 $2l_N \leqslant N' < N$. 根据引理 2,

$$l_{N'+1} \geqslant N'+1-l_{N'}.$$

但是显然有 $l_{N'} = l_{2l_N}$, 又因 $N' \geqslant 2l_N$ 和 $l_{2l_N} \leqslant l_N$, 所以

$$l_{N'+1} \geqslant 2l_N+1-l_N > l_N.$$

可是 $N'+1 \leqslant N$, 因此上式与 l_n 的单调不减性相矛盾. 这证明了 $\langle f_{2l_N}(x), l_{2l_N}\rangle$ 产生(1).

既然 $\langle f_{2l_N}(x), l_{2l_N}\rangle$ 产生(1), $l_{2l_N} \leqslant l_N$, 而 $\langle f_N(x), l_N\rangle$ 是产生(1)的最短线性移位寄存器, 所以一定有

$$\langle f_{2l_N}(x), l_{2l_N}\rangle = \langle f_N(x), l_N\rangle.$$

这证明了系理 1.

系理 2　设

$$a_0,\ a_1,\ a_2,\ \cdots \tag{16}$$

是一个 q 元周期序列, 并假定它的周期等于 N, 那么按综合算法算出的 $\langle f_{2N}(x), l_{2N}\rangle$ 就是产生它的唯一的那个最短线性

移位寄存器，而 $f_{2N}(x)$ 就是它的极小多项式. 更进一步，如果 $\partial^0 f_{2N}(x)=n$，那么按综合算法算出的 $f_{2n}(x)$ 就是它的极小多项式，而

$$f_{2n}(x)=f_{2n+1}(x)=f_{2n+2}(x)=\cdots=f_{2N}(x)=\cdots. \quad (17)$$

证. 令 $f(x)=1-x^N$. 显然 $\langle f(x), N\rangle$ 是产生(16)的一个线性移位寄存器. 特别, $\langle f(x), N\rangle$ 产生(16)的前 $2N$ 项. 因此产生(16)的前 $2N$ 项的最短线性移位寄存器的级数 $l_{2N}\leqslant N$. 那么根据定理 2 可知，产生(16)的前 $2N$ 项的最短线性移位寄存器是唯一的. 于是按综合算法算出的 $\langle f_{2N}(x), l_{2N}\rangle$ 就是产生(16)的前 $2N$ 项的唯一的那个最短线性移位寄存器. 因为(16)是周期等于 N 的周期序列，而 $l_{2N}\leqslant N$，所以 $\langle f_{2N}(x), l_{2N}\rangle$ 不仅产生(16) 的前 $2N$ 项，而且可以产生整个序列(16). 由此推出产生(16)的最短线性移位寄存器的级数一定 $\leqslant l_{2N}$，因而 $\leqslant N$. 但产生(16)的任一最短线性移位寄存器也一定能产生(16)的前 $2N$ 项，那么根据唯一性可知它一定就是 $\langle f_{2N}(x), l_{2N}\rangle$. 这证明了 $\langle f_{2N}(x), l_{2N}\rangle$ 是产生(16)的唯一的那个最短线性移位寄存器.

我们再证明 $f_{2N}(x)$ 就是(16)的极小多项式. 写

$$f_{2N}(x)=1+c_1x+c_2x^2+\cdots+c_{l_{2N}}x^{l_{2N}}.$$

如果 $c_{l_{2N}}\neq 0$，$f_{2N}(x)$ 就是(16)的极小多项式. 因此问题是要证明 $c_{l_{2N}}\neq 0$. 假定 m 是最大的正整数使

$$c_m\neq 0,\ c_{m+1}=c_{m+2}=\cdots=c_{l_{2N}}=0,$$

那么 $m\leqslant l_{2N}$，而

$$f_{2N}(x)=1+c_1x+c_2x^2+\cdots+c_mx^m.$$

于是 $\langle f_{2N}(x), m\rangle$ 就产生将(16)的前 $l_{2N}-m$ 项略去后所得的序列

$$a_{l_{2N}-m},\ a_{l_{2N}-m+1},\ a_{l_{2N}-m+2},\ \cdots$$

因而更能产生将(16)的前 N 项略去后所得的序列

$$a_N,\ a_{N+1},\ a_{N+2},\ \cdots \tag{18}$$

因 (16) 是周期等于 N 的周期序列，所以序列 (18) 实际上就是(16). 这证明了 $\langle f_{2N}(x),\ m\rangle$ 也能产生(16). 但 $\langle f_{2N}(x),\ l_{2N}\rangle$ 是产生 (16) 的最短线性移位寄存器，而 $m\leqslant l_{2N}$，所以一定有 $m=l_{2N}$. 这证明了 $c_{l_{2N}}\neq 0$.

更进一步，再假定 $\partial^0 f_{2N}(x)=n$，即 $l_{2N}=n$. 根据系理 1，$\langle f_{2n}(x),\ l_{2n}\rangle$ 就是产生 (16) 的前 $2N$ 项的唯一的那个最短线性移位寄存器. 因此一定有 $\langle f_{2n}(x),\ l_{2n}\rangle=\langle f_{2N}(x),\ n\rangle$. 特别 $f_{2n}(x)=f_{2N}(x)$. 所以 $f_{2n}(x)$ 就是 (16) 的极小多项式，由此立刻推出(17)成立.

系理 2 有下面这个重要的特例：

系理 3 设

$$a_0,\ a_1,\ a_2,\ \cdots$$

是一个周期等于 q^n-1 的 q 元 m 序列，那么按综合算法求得的 $f_{2n}(x)$ 就是产生它的本原多项式.

有了系理 3 我们就可以明白为什么在例 2 中

$$f_8(x)=f_9(x)=\cdots=f_{15}(x)=1+x^3+x^4.$$

实际上，算出了 $f_8(x)$ 就不必再算下去了，$f_8(x)$ 就是产生例 1 中周期 15 的 m 序列的本原多项式.

还应该指出的是，从系理 2 可知，综合算法还提供了求产生任一给定的 q 元周期序列(特别是二元伪随机序列)的极小多项式的一个算法. 这就是说，综合算法提供了上节末尾所提的问题，即如何用硬件产生一给定的伪随机序列这个问题，一个解法. 因为一旦给定的伪随机序列的极小多项式能够求出，就可构造产生这个伪随机序列的线性移位寄存器.

例 3 求周期等于 11 的二次剩余序列

$$0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\cdots$$

的极小多项式.

在例1中，我们已经按综合算法算出了产生周期11的二次剩余序列前11项（即一个周期）的最短线性移位寄存器．按综合算法继续算下去，算到第22步．将计算过程列表如下：

表 3

步数 (n)	d_{n-1}	f_n	l_n
12	1	$1+x^4+x^5+x^6$	6
13	1	$1+x^3+x^5+x^6+x^7$	7
14	1	$1+x+x^3$	7
15	1	$1+x+x^2+x^3+x^6+x^7+x^8$	8
16	1	$1+x^3+x^4+x^6+x^7+x^8$	8
17	1	$1+x^2+x^4+x^5+x^6+x^7+x^8$	9
18	1	$1+x+x^2+x^6+x^9$	9
19	0	$1+x+x^2+x^6+x^9$	9
20	1	$1+x+x^2+x^3+x^7+x^{10}+x^{11}$	11
21	1	$1+x^{11}$	11
22	0	$1+x^{11}$	11

因此，周期等于11的二次剩余序列的极小多项式是 $1+x^{11}$．

当 $2l_N>N$ 时，根据定理2，产生(1)的最短线性移位寄存器并不唯一．但却可以很容易地从用综合算法求得的产生(1)的那个最短线性移位寄存器 $\langle f_N(x), l_N\rangle$ 得出产生(1)的所有的最短线性移位寄存器．

定理3 任给一个长为 N 的 q 元序列(1)，并设产生它的前 n 项的最短线性移位寄存器的级数是 $l_n(1\leqslant n\leqslant N)$．假定 $2l_N>N$，并设 $m(0\leqslant m<N)$ 是个正整数使

$$l_m<l_{m+1}=l_{m+2}=\cdots=l_N.$$

再设 $\langle f_N(x), l_N\rangle$ 是按综合算法求出的产生(1)的最短线性移位寄存器，而 $f_m(x)$ 是按综合算法求出的产生(1)的前 m 项的最短线性移位寄存器的联接多项式，那么

$$\{\langle f_N(x)+q(x)x^{N-m}f_m(x),\ l_N\rangle\},$$

其中 $q(x)$ 是任意一个次数 $<2l_N-N$ 的多项式，就是所有产生(1)的最短线性移位寄存器所组成的集合.

证. 设 $\langle f(x),\ l_N\rangle$ 是产生 (1) 的任意一个最短线性移位寄存器. 写

$$f(x)=1+c_1x+c_2x^2+\cdots+c_{l_N}x^{l_N},$$

那么 $$a_k=-\sum_{i=1}^{l_N}c_ia_{k-i},\ k=l_N,\ l_N+1,\ \cdots,\ N-1.$$

递归地定义

$$a_k=-\sum_{i=1}^{l_N}c_ia_{k-i},\ k=N,\ N+1,\ \cdots,\ 2l_N-1.$$

那么根据定理 2, $\langle f(x),\ l_N\rangle$ 就是唯一的那个产生长为 $2l_N$ 的 q 元序列

$$a_0,\ a_1,\ a_2,\ \cdots,\ a_{N-1},\ a_N,\ a_{N+1},\ \cdots,\ a_{2l_N-1} \tag{19}$$

的最短线性移位寄存器. 更进一步, 如果 $\langle f(x),\ l_N\rangle$ 和 $\langle f_1(x),\ l_N\rangle$是两个不同的产生(1)的最短线性移位寄存器, 那么仍根据定理 2, 它们从初始状态 $(a_0,\ a_1,\ \cdots,\ a_{l_N-1})$ 出发所产生的长为 $2l_N$ 的 q 元序列一定不同. 因此产生 (1) 的 l_N 级线性移位寄存器的个数 $\leqslant$ 前 N 项是(1)的长为 $2l_N$ 的 q 元序列的个数, 而后者显然等于 q^{2l_N-N}.

另一方面, 任意添 $\mathbf{F}_q$ 中 $2l_N-N$ 个元素 $b_N,\ b_{N+1},\ \cdots,\ b_{2l_N-1}$ 到(1)的后面, 得到一个长为 $2l_N$ 的 q 元序列

$$a_0,\ a_1,\ a_2,\ \cdots,\ a_{N-1},\ b_N,\ b_{N+1},\ \cdots,\ b_{2l_N-1}. \tag{20}$$

因 $2l_N>N$, 从引理 4 可以推出, 产生 (20) 的最短线性移位寄存器也是 l_N 级的. 当 $b_N,\ b_{N+1},\ \cdots,\ b_{2l_N-1}$ 独立地取 $\mathbf{F}_q$ 中 q 个元素时, 一共得到 q^{2l_N-N} 个长为 $2l_N$ 的 q 元序列(20). 产生这 q^{2l_N-N} 个长为 $2l_N$ 的 q 元序列的最短线性移位寄存器都是 l_N 级的, 那么根据定理 2, 它们一定两两不同. 它们当然都产

生(1). 这样一共得到 q^{2l_N-N} 个产生(1)的最短线性移位寄存器. 上一段已经证明, 产生 (1) 的最短线性移位寄存器的个数 $\leqslant q^{2l_N-N}$. 因此产生(1)的最短线性移位寄存器的个数恰好等于 q^{2l_N-N}.

仍设 $\langle f(x), l_N\rangle$ 是产生 (1) 的任意一个最短线性移位寄存器, 并设它从初始状态 $(a_0, a_1, \cdots, a_{l_N-1})$ 出发产生的序列的前 $2l_N$ 项是(19), 那么按综合算法求产生(19)的最短线性移位寄存器时, 因 $2l_N>N$, 根据引理 4 总有

$$l_m<l_{m+1}=l_{m+2}=\cdots=l_N=l_{N+1}=\cdots=l_{2l_N}.$$

因此当按综合算法计算的某一个 $d_n\neq 0(N\leqslant n\leqslant 2l_N-1)$ 时, 按综合算法从 $f_n(x)$ 递归地得出的 $f_{n+1}(x)$ 只是在原来的 $f_n(x)$ 上添上了 $f_m(x)$ 的一个陪式 $-d_nd_m^{-1}x^{n-m}f_m(x)$, 而

$$-d_nd_m^{-1}x^{n-m}f_m(x)=(-d_nd_m^{-1}x^{n-N})(x^{N-m}f_m(x)).$$

所以按综合算法最后得到的产生(19)的最短线性移位寄存器必有形状

$$\langle f_N(x)+q(x)x^{N-m}f_m(x), l_N\rangle,$$

其中 $\partial^0 q(x)<2l_N-N$. 根据定理 2, 产生(19)的最短线性移位寄存器是唯一的, 所以 $f(x)$ 必为形状

$$f_N(x)+q(x)x^{N-m}f_m(x),\quad \partial^0 q(x)<2l_N-N \tag{21}$$

的多项式. 但形状(21)的多项式总共 q^{2l_N-N} 个. 所以形状(21)的 q^{2l_N-N} 个多项式就是产生 (1) 的 q^{2l_N-N} 个最短线性移位寄存器的联接多项式.

这样定理 3 就完全证明了.

最后, 我们再对综合算法作一个注记. 综合算法的第2.2)步里要求逆元素 d_m^{-1}. 但只要将综合算法略加修饰, 就可以减成只求一个逆元素.

修饰的综合算法 任给一个长为 N 的 q 元序列 (1). 对 n 用数学归纳法来定义一系列多项式 $g_n(x)$ 和一系列非负

整数 $l'_n(n=1, 2, \cdots, N)$, 而 $\partial^0 g_n(x)\leqslant l'_n$.

(1) 设 n_0 是个非负整数使

$$a_1=a_2=\cdots=a_{n_0-1}=0,\ a_{n_0}\neq 0,$$

那么约定 $$D_1=D_2=\cdots=D_{n_0-1}=0,\ D_{n_0}=a_{n_0},$$

并令 $$g_1(x)=g_2(x)=\cdots=g_{n_0}(x)=1,$$

$$l'_1=l'_2=\cdots=l'_{n_0}=0,$$

$$g_{n_0+1}(x)=1-D_{n_0}x^{n_0+1},\ l'_{n_0+1}=n_0+1.$$

(2) 设 $g_i(x)$, l'_i, $i=1, 2, \cdots, n(n_0<n<N)$ 已求得, 而 $\partial^0 g_i(x)\leqslant l'_i$,

$$l'_1=l'_2=\cdots=l'_{n_0}<l'_{n_0+1}\leqslant l'_{n_0+2}\leqslant\cdots\leqslant l'_n.$$

令 $$g_n(x)=b_{n0}+b_{n1}x+b_{n2}x^2+\cdots+b_{nl'_n}x^{l'_n}.$$

计算 $$D_n=b_{n0}a_n+b_{n1}a_{n-1}+b_{n2}a_{n-2}+\cdots+b_{nl'_n}a_{n-l'_n}.$$

区别下面两个情形:

2.1) $D_n=0$. 这时令

$$g_{n+1}(x)=g_n(x),\ l'_{n+1}=l'_n.$$

2.2) $D_n\neq 0$. 这时有 $m(0\leqslant m<n)$ 使

$$l'_m<l'_{m+1}=l'_{m+2}=\cdots=l'_n$$

那么令 $$g_{n+1}(x)=D_m g_n(x)-D_n x^{n-m}g_m(x),$$

$$l'_{n+1}=\max\{l'_n,\ n+1-l'_n\}.$$

最后我们得到 $g_N(x)$ 和 l'_n. 写

$$g_N(x)=b_{N0}+b_{N1}x+b_{N2}x^2+\cdots+b_{Nl'_N}x^{l'_N},$$

那么可以证明 $b_{N0}\neq 0$, 而 $\langle b_{N0}^{-1}g(x),\ l'_N\rangle$ 就是产生(1)的最短线性移位寄存器.

为了证明这一事实, 我们先平行于修饰的综合算法定义一系列的 $\mathbf{F}_q$ 中的元素 δ_n, $n=1, 2, \cdots, N$:

(1) 设 n_0 是个非负整数使

$$a_1=a_2=\cdots=a_{n_0-1}=0,\ a_{n_0}\neq 0,$$

那么定义 $$\delta_1=\delta_2=\cdots=\delta_{n_0}=\delta_{n_0+1}=1.$$

(2) 设 $\delta_1, \cdots, \delta_n(n_0<n<N)$ 已定义，区别 2.1) 和 2.2) 两种情况.

2.1) 即 $D_n=0$ 的情况. 这时定义

$$\delta_{n+1}=1.$$

2.2) 即 $D_n\neq 0$ 的情况. 这时定义

$$\delta_{n+1}=D_m.$$

我们可以证明

定理 4 对 $n=1, 2, \cdots, N$, 我们有

$$l'_n=l_n,$$

$$g_n(x)=\left(\prod_{i=1}^{n}\delta_i\right)f_n(x),$$

$$D_n=\left(\prod_{i=1}^{n}\delta_i\right)d_n\ (n\neq N).$$

特别, $g_n(x)$ 的零次项 $\prod_{i=1}^{n}\delta_i\neq 0$.

证. 对 n 用归纳法来证明本定理.

设 n_0 是非负整数使

$$a_1=a_2=\cdots=a_{n_0-1}=0,\ a_{n_0}\neq 0,$$

那么根据综合算法和修饰的综合算法

$$f_1(x)=f_2(x)=\cdots=f_{n_0}(x)=1,$$

$$l_1=l_2=\cdots=l_{n_0}=0,$$

$$d_1=d_2=\cdots=d_{n_0-1}=0,\ d_{n_0}=a_{n_0},$$

$$f_{n_0+1}(x)=1-d_{n_0}x^{n_0+1},\ l_{n_0+1}=n_0+1,$$

$$g_1(x)=g_2(x)=\cdots=g_{n_0}(x)=1,$$

$$l'_1=l'_2=\cdots=l'_{n_0}=0,$$

$$D_1=D_2=\cdots=D_{n_0-1}=0,\ D_{n_0}=a_{n_0},$$

$$g_{n_0+1}(x)=1-D_{n_0}x^{n_0+1},\ l'_{n_0+1}=n_0+1.$$

根据 δ_n 的定义,

$$\delta_1=\delta_2=\cdots=\delta_{n_0}=\delta_{n_0+1}=1.$$

容易看出来本定理对于 $n\leqslant n_0+1$ 成立.

设 $n_0<n<N$, 并假定本定理对于 1, 2, …, n 都成立. 我们去证明它对于 $n+1$ 也成立.

当 $d_n=0$ 时, 根据归纳法假设从 $D_n=\left(\prod_{i=1}^{n}\delta_i\right)d_n$ 推出 $D_n=0$. 根据综合算法, 修饰的综合算法及 δ_{n+1} 的定义方法, 有

$$f_{n+1}(x)=f_n(x),\ l_{n+1}=l_n,$$
$$g_{n+1}(x)=g_n(x),\ l'_{n+1}=l'_n,\ \delta_{n+1}=1,$$

那么根据归纳法假设就推出

$$l'_{n+1}=l'_n=l_n=l_{n+1},$$
$$g_{n+1}(x)=g_n(x)$$
$$=\left(\prod_{i=1}^{n}\delta_n\right)f_n(x)=\left(\prod_{i=1}^{n+1}\delta_i\right)f_{n+1}(x). \tag{22}$$

仍根据归纳法假设 $g_n(x)$ 的零次项 $\prod_{i=1}^{n}\delta_i\neq 0$, 而 $\delta_{n+1}\neq 0$, 所以 $g_{n+1}(x)$ 的零次项 $\prod_{i=1}^{n+1}\delta_i\neq 0$. 比较 (22) 式双方同次项系数得

$$b_{n+10}=\prod_{i=1}^{n+1}\delta_i,\ b_{n+1j}=\left(\prod_{i=1}^{n+1}\delta_i\right)c_{n+1j},\ j=1,\ 2,\ \cdots,\ l_{n+1}.$$

由此立刻推出

$$D_{n+1}=b_{n+10}a_n+b_{n+11}a_{n-1}+b_{n+12}a_{n-2}+\cdots+b_{n+1l_N}a_{n-l_{N+1}}$$
$$=\left(\prod_{i=0}^{n+1}\delta_i\right)(a_n+c_{n+11}a_{n-1}+c_{n+12}a_{n-2}+\cdots+c_{n+1l_{N+1}}a_{n-l_{N+1}})$$
$$=\left(\prod_{i=0}^{n+1}\delta_i\right)d_{n+1}.$$

当 $d_n\neq 0$ 时, 根据归纳法假设必有 $D_n\neq 0$. 这时有 $m(0\leqslant m<n)$ 使

$$l_m<l_{m+1}=l_{m+2}=\cdots=l_n,$$

那么根据综合算法，修饰的综合算法和 δ_{n+1} 的定义方法，

$$f_{n+1}(x)=f_n(x)-\hat{d}_n d_m^{-1}x^{n-m}f_m(x),$$

$$l_{n+1}=\max\{l_n,\ n+1-l_n\},$$

$$g_{n+1}(x)=D_m g_n(x)-D_n x^{n-m}g_m(x),$$

$$l'_{n+1}=\max\{l'_n,\ n+1-l'_n\},$$

$$\delta_{n+1}=D_m.$$

根据归纳法假设就推出

$$l'_{n+1}=l_{n+1}$$

$$\begin{aligned}g_{n+1}(x)&=D_m g_n(x)-D_n x^{n-m}g_m(x)\\&=\delta_{n+1}\left(\prod_{i=1}^{n}\delta_i\right)f_n(x)-\left(\prod_{i=1}^{n}\delta_i\right)d_n x^{n-m}\left(\prod_{i=1}^{m}\delta_i\right)f_m(x)\\&=\left(\prod_{i=1}^{n+1}\delta_i\right)(f_n(x)-d_n d_m^{-1}x^{n-m}f_m(x))\\&=\left(\prod_{i=1}^{n+1}\delta_i\right)f_{n+1}(x).\end{aligned}$$

和上一情形一样可以证明 $g_{n+1}(x)$ 的零次项 $\prod_{i=0}^{n+1}\delta_i\neq 0$ 以及

$$D_{n+1}=\left(\prod_{i=0}^{n+1}\delta_i\right)d_{n+1}.$$

这证明了定理 4 对 $n+1$ 也成立.

根据数学归纳法可知定理 4 对 $n=1, 2, \cdots, N$ 都成立.

由定理 4 立刻推出

$$b_{N0}^{-1}g_N(x)=\left(\prod_{i=1}^{N}\delta_i\right)^{-1}g_N(x)=f_N(x).$$

因此 $\langle b_{N0}^{-1}g_N(x),\ l_N\rangle$ 就是产生(1)的最短线性移位寄存器.

§9 非线性移位寄存器介绍

上一节介绍了求产生给定的伪随机序列的最短线性移位

寄存器的一个综合算法．用这个方法求得的线性移位寄存器的级数可能很大，这样技术上实现起来就会有困难，因此我们在这一节里再介绍另外的用硬件来产生给定的伪随机序列的方法．这些方法要用到非线性移位寄存器．我们就先来介绍非线性移位寄存器．

下面是 n 级(反馈)移位寄存器的框图：

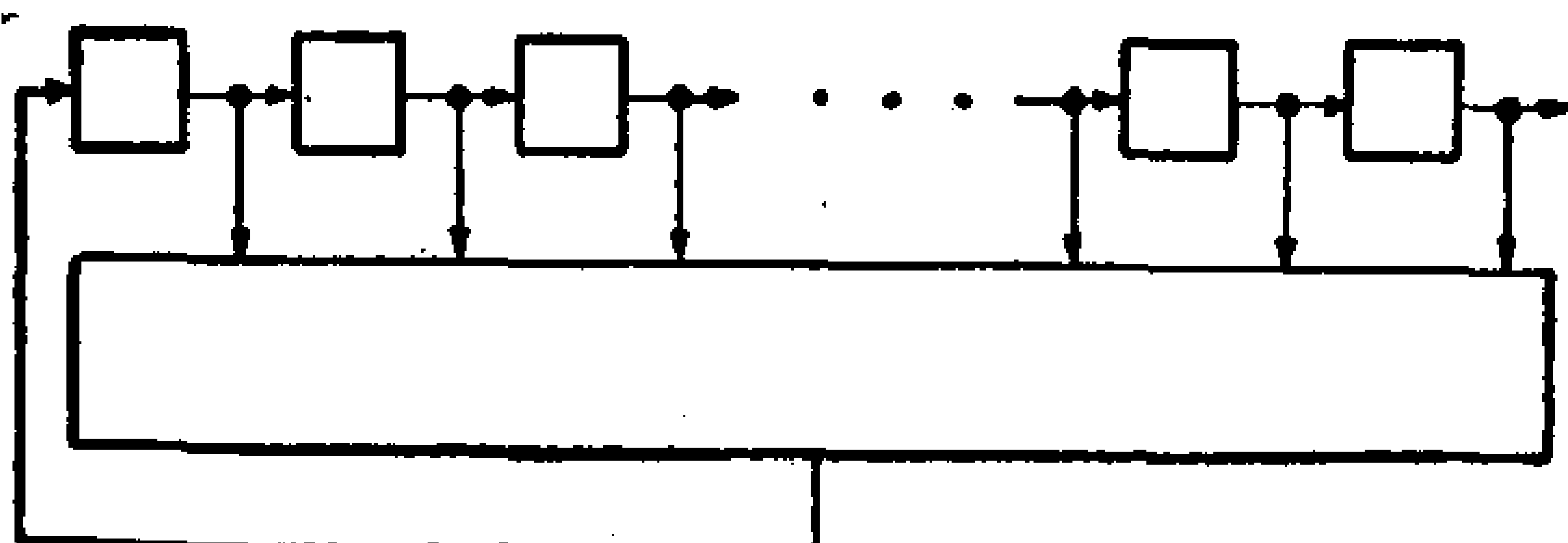


图 1

上面一排小方框一共 n 个，代表 n 个寄存器，把它们从左往右依序叫做第1级寄存器，第2级寄存器，……，第 n 级寄存器，每个寄存器可以取0和1这两种状态之一，而0和1恒看作 $\mathbf{F}_2$ 的元素．下面的长方框代表一个有 n 个输入端和一个输出端的开关线路(也叫组合线路) C．假定开始时(即时刻0时)，第1级寄存器的状态是 a_{n-1}，第2级寄存器的状态是 a_{n-2}，…，第 n 级寄存器的状态是 a_0．我们就说这个移位寄存器的初始状态是 $(a_0, a_1, \cdots, a_{n-1})$．当加上一个移位脉冲后，一方面每个寄存器的内容(0或1)移给下一级，最末一级(第 n 级)的内容即为输出；另一方面将这个 n 级寄存器的内容输送给开关线路 C 的 n 个输入端并将 C 的输出，设为 a_n，输送到第1级寄存器，因此 C 又叫这个移位寄存器的*反馈开关线路*．这样，在时刻1(即加上一个移位脉冲后)，这个移位寄存器的状态就是 $(a_1, a_2, \cdots, a_n)$，而输出是 a_0．注意这里 a_n 是由这个移位寄存器在时刻0的状态 $(a_0, a_1, \cdots, a_{n-1})$ 和反馈开关线路 C 唯一确定的．再加上一个移位脉冲后，即在时刻2，这

个移位寄存器的状态就是$(a_2, a_3, \cdots, a_{n+1})$，而输出是$a_1$，这里$a_{n+1}$是当开关线路$C$的$n$个输入端从右往左依序是$a_1$, $a_2 \cdots, a_n$时，它的输出的值，因而是由时刻1的状态$(a_1, a_2, \cdots, a_n)$和反馈开关线路C唯一确定. 这样不断地加移位脉冲，上述移位寄存器的输出就是一个二元序列

$$a_0, a_1, a_2, \cdots,$$

这个序列由这个移位寄存器的初始状态$(a_0, a_1, \cdots, a_{n-1})$和反馈开关线路$C$所唯一确定，叫做这个移位寄存器、从初始状态$(a_0, a_1, \cdots, a_{n-1})$出发产生的(反馈)移位寄存器序列.

一个n级移位寄存器的功能由它的反馈开关线路所确定. 在数学上这个有n个输入端和一个输出端的开关线路，可以由一个n元开关函数$f(x_1, x_2, \cdots, x_n)$来描述，它是一个n个变元$x_1, x_2, \cdots, x_n$可以独立地任取0和1这两个可能的值，而函数值$f(x_1, x_2, \cdots, x_n)$也只能取0或1为值的函数. 这样，当上述n级移位寄存器的状态是$(a_1, a_2, \cdots, a_n)$时，即当它的第i级寄存器的内容是$a_{n-i+1}(i=1, 2, \cdots, n)$时，加上一个移位脉冲，它的反馈开关线路的$n$个输入端从右往左依序是$a_1, a_2, \cdots, a_n$，而输出端(也即第1级寄存器的内容)是$f(a_1, a_2, \cdots, a_n)$. 描述一个$n$级移位寄存器的反馈开关函数又叫这个移位寄存器的反馈函数，有时也叫反馈逻辑，因此一个n级移位寄存器的功能由它的反馈函数所完全确定. 以$f(x_1, x_2, \cdots, x_n)$为反馈函数的n级移位寄存器的反馈开关线路往往记作C_f.

例如§1例1中的移位寄存器的反馈逻辑是

$$f(x_1, x_2, x_3, x_4)=x_1+x_2+x_3+x_4$$

而§1例2中的移位寄存器的反馈逻辑是

$$f(x_1, x_2, x_3, x_4)=x_1+x_2.$$

一个n元开关函数$f(x_1, x_2, \cdots, x_n)$可以由它的真值表

来描述. 下面是两个4元开关函数的真值表:

表 1

$x_1x_2x_3x_4$	$f_1(x_1, x_2, x_3, x_4)$	$x_1x_2x_3x_4$	$f_2(x_1, x_2, x_3, x_4)$
0 0 0 0	0	0 0 0 0	1
0 0 0 1	1	0 0 0 1	0
0 0 1 0	1	0 0 1 0	0
0 0 1 1	0	0 0 1 1	0
0 1 0 0	1	0 1 0 0	0
0 1 0 1	0	0 1 0 1	0
0 1 1 0	0	0 1 1 0	1
0 1 1 1	1	0 1 1 1	1
1 0 0 0	1	1 0 0 0	1
1 0 0 1	0	1 0 0 1	0
1 0 1 0	0	1 0 1 0	0
1 0 1 1	1	1 0 1 1	0
1 1 0 0	0	1 1 0 0	0
1 1 0 1	1	1 1 0 1	0
1 1 1 0	1	1 1 1 0	1
1 1 1 1	0	1 1 1 1	1

注意在上面的真值表中, x_1, x_2, x_3, x_4 取的16种值是按字典次序排列的; 即规定$0<1$, 而我们把$a_1a_2a_3a_4$排在$b_1b_2b_3b_4$的前面, 如果

$a_1<b_1$,

或 $a_1=b_1$, 而 $a_2<b_2$,

或 $a_1=b_1$, 而 $a_2=b_2$, $a_3<b_3$,

或 $a_1=b_1$, $a_2=b_2$, $a_3=b_3$, 而 $a_4<b_4$.

对于n元开关函数$f(x_1, x_2, \cdots, x_n)$的真值表中, x_1, x_2, $\cdots$, x_n取的2^n种值, 也是按字典次序排列的.

显然, 一共有2^{2^n}个n元开关函数. 以不同的n元开关函数为反馈函数的n级移位寄存器的功能两两不同, 因此一共

有 2^{2^n} 个功能两两不同的 n 级移位寄存器.

下面我们再介绍 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 的两种表示方法. 先按照下面的真值表规定一个开关函数 $\bar{x}$:

表 2

x	$\bar{x}$
0	1
1	0

我们约定 $$x^1=x,\ x^0=\bar{x}.$$
那么对任意 n 个值 $c_1, c_2, \cdots, c_n$($c_i=0$ 或 1), 我们有 n 元开关函数

$$x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}, \tag{1}$$

这个 n 元开关函数只在 $(c_1, c_2, \cdots, c_n)$ 处取值 1, 而在其余各点均取值 0. 我们把 n 元开关函数(1)叫做一个小项.

这样我们可以把任意一个 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 唯一地表成小项的和

$$f(x_1, x_2, \cdots, x_n) = \sum_{c_1, c_2, \cdots, c_n=0}^{1} f(c_1, c_2, \cdots, c_n) x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}, \tag{2}$$

其次, 我们有

$$\bar{x}=x+1.$$

将 $\bar{x}_i=x_i+1(1\leqslant i\leqslant n)$ 代入(2), 并注意到

$$x\cdot x=x,\ x\cdot y=y\cdot x,$$

于是又可以将 $f(x_1, x_2, \cdots, x_n)$ 唯一地表成以下的多项式形状:

$$f(x_1, x_2, \cdots, x_n)=\sum_{r=0}^{n}\ \sum_{1\leqslant i_1<i_2<\cdots<i_r\leqslant n} c_{i_1i_2\cdots i_r}x_{i_1}x_{i_2}\cdots x_{i_r}, \tag{3}$$

其中 $c_{i_1i_2\cdots i_r}=0$ 或 1, 而当 $r=0$ 时我们约定 $x_{i_1}x_{i_2}\cdots x_{i_r}=1$.

(2) 叫做 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 的小项表示，而(3)叫做它的多项式表示。当 $f(x_1, x_2, \cdots, x_n)$ 的多项式表示是 $x_1, x_2, \cdots, x_n$ 的线性齐次多项式时，即

$$f(x_1, x_2, \cdots, x_n)=c_1x_1+c_2x_2+\cdots+c_nx_n,\ c_i=0\text{ 或 }1,$$

以 $f(x_1, x_2, \cdots, x_n)$ 为反馈逻辑的 n 级移位寄存器就是前面讨论的 n 级线性移位寄存器，否则就叫 n 级非线性移位寄存器。

如果 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 的取值与 x_1 的取值无关，即

$$f(0, x_2, \cdots, x_n)=f(1, x_2, \cdots, x_n),$$

我们就说 f 是退化的，否则是非退化的。当 f 是退化时，如令

$$g(x_1, x_2, \cdots, x_{n-1})=f(0, x_1, x_2, \cdots, x_{n-1}),$$

那么 $g(x_1, x_2, \cdots, x_{n-1})$ 就是个 $n-1$ 元开关函数，它的真值表可以从 $f(x_1, x_2, \cdots, x_n)$ 的真值表划去第 1 列和后 2^{n-1} 行并将 $x_2, \cdots, x_n$ 依序改记成 $x_1, \cdots, x_{n-1}$ 而得，例如，前面举的 $f_2(x_1, x_2, \cdots, x_n)$ 就是退化的，而

$$g(x_1, x_2, x_3)=f_2(0, x_1, x_2, x_3)$$

的真值表即是

表 3

$x_1\ x_2\ x_3$	$g(x_1, x_2, x_3)$
0 0 0	1
0 0 1	0
0 1 0	0
0 1 1	0
1 0 0	0
1 0 1	0
1 1 0	1
1 1 1	1

当 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 退化时，令

$$g(x_1, x_2, \cdots, x_{n-1})=f(0, x_1, x_2, \cdots, x_{n-1}),$$

那么以 $f(x_1, x_2, \cdots, x_n)$ 为开关函数的开关线路 C_f 可以看作是有 $n-1$ 个输入端和一个输出端的开关线路 C_g. 这时以 $f(x_1, x_2, \cdots, x_n)$ 为反馈逻辑的 n 级移位寄存器从初始状态 $(a_0, a_1, \cdots, a_{n-1})$ 出发产生的移位寄存器序列与以 $g(x_1, x_2, \cdots, x_{n-1})$ 为反馈逻辑的 $n-1$ 级移位寄存器从初始状态 $(a_1, a_2, \cdots, a_{n-1})$ 出发产生的移位寄存器序列，除相差 a_0 这一项以外，完全一样. 因此这时可以说以 $f(x_1, x_2, \cdots, x_n)$ 为反馈逻辑的 n 级移位寄存器是退化的，即退化成以 $g(x_1, x_2, \cdots, x_{n-1})$ 为反馈逻辑的 $n-1$ 级移位寄存器.

今后我们谈到移位寄存器，总假定它是非退化的，即它的反馈函数是非退化的.

对于任一移位寄存器，也可以像 §3 中对于线性移位寄存器一样地引进状态图. 设有一个 n 级移位寄存器，它的反馈逻辑是 $f(x_1, x_2, \cdots, x_n)$. 用 G_f 表示它的状态图，它是一个有 2^n 个顶点和 2^n 条弧的一个有向图，顶点集是

$$V_n(\mathbf{F}_2)=\{(a_1, a_2, \cdots, a_n)\,|\,a_1, a_2, \cdots, a_n\in\mathbf{F}_2\},$$

每个顶点代表一个状态. 每个顶点 $(a_1, a_2, \cdots, a_n)$ 是唯一一条弧的起点，这条弧的终点是 $(a_2, \cdots, a_n, f(a_1, a_2, \cdots, a_n))$. 显然，这个移位寄存器的反馈逻辑，因而它的功能，由它的状态图 G_f 唯一确定. G_f 还确定这个移位寄存器的状态转移变换 T_f:

$$T_f\colon (a_1, a_2, \cdots, a_n)\to(a_2, \cdots, a_n, f(a_1, a_2, \cdots, a_n)),$$

反过来，G_f 也由 T_f 所确定.

下面我们画出以表 1 中的 $f_1(x_1, x_2, x_3, x_4)$ 和表 3 中的 $g(x_1, x_2, x_3)$ 为反馈逻辑的移位寄存器的状态图.

我们看到，$f_1(x_1, x_2, x_3, x_4)$ 的状态图由 4 个圈组成；而

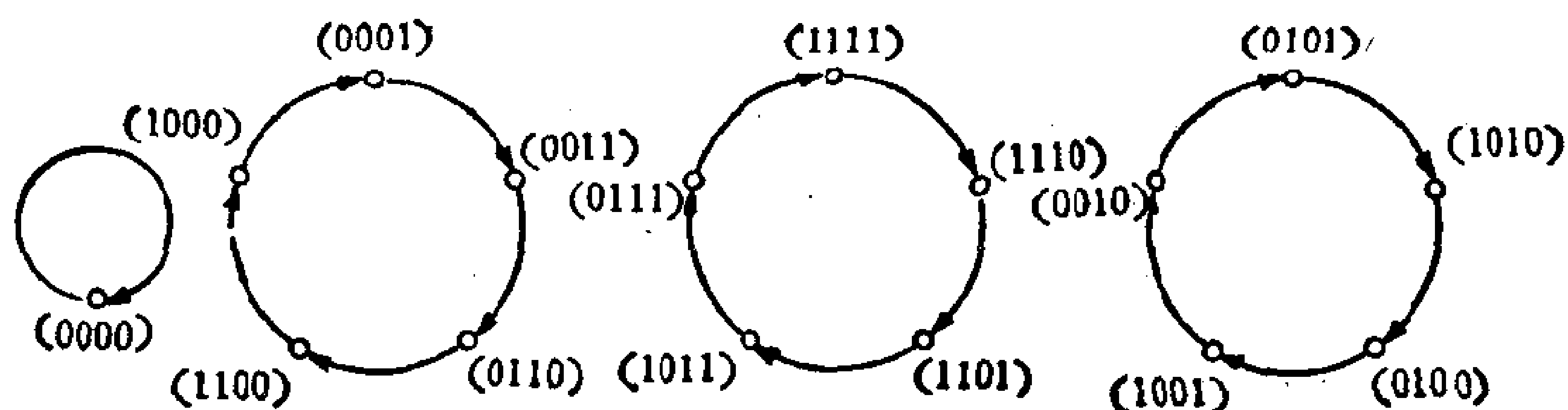


图 2 $f(x_1, x_2, x_3, x_4)$ 的状态图

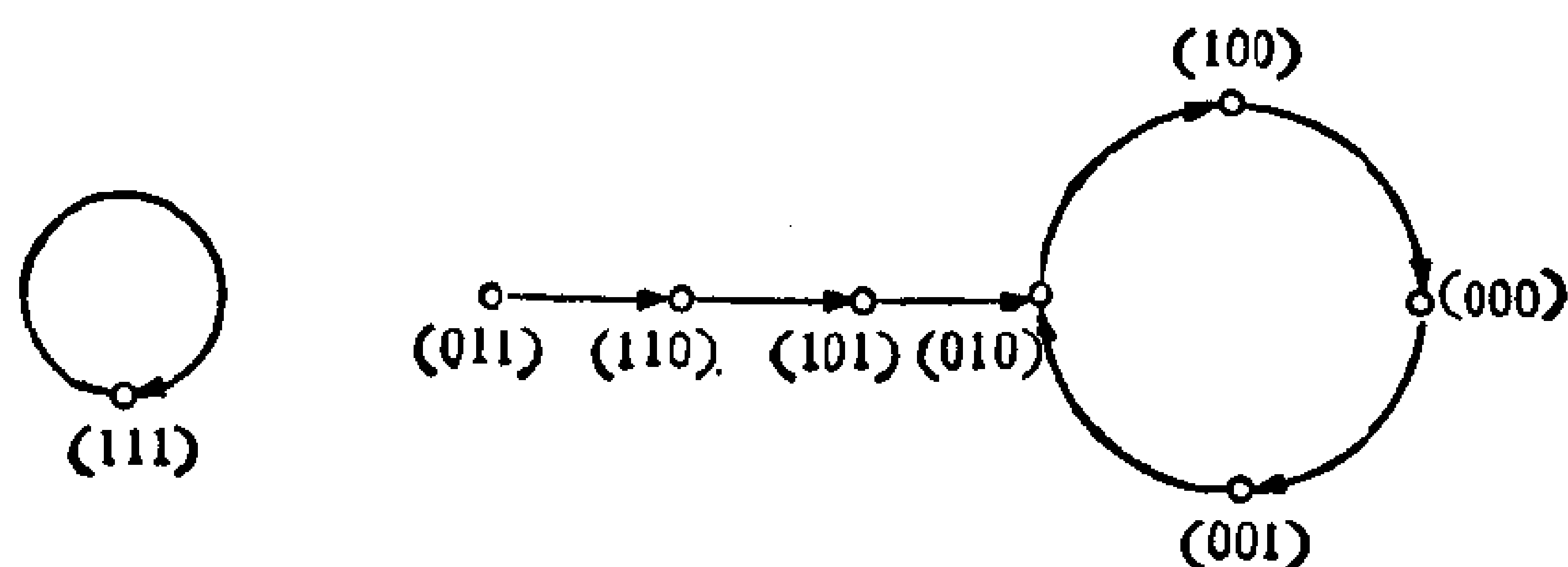


图 3 $g(x_1, x_2, x_3)$ 的状态图

$g(x_1, x_2, x_3)$ 的状态图除了有两个圈以外，还有枝．一般我们有：

定理 1 n 级移位寄存器的状态图一定有圈．实际上，从 n 级移位寄存器的任一状态 $\mathbf{s}_0=(a_0, a_1, \cdots, a_{n-1})$ 出发，连续施行状态转移变换 T_f，得到一系列的状态

$$\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \cdots, \tag{4}$$

其中 $\mathbf{s}_k=T_f\mathbf{s}_{k-1}=(a_k, a_{k+1}, \cdots, a_{k+n-1})$，

那么总存在一个最小的正数 $n_1<2^n+1$ 使得 $\mathbf{s}_{n_1}$ 与足码比它小的一个状态，设为 $\mathbf{s}_{n_0}(n_0<n_1)$ 相等．$\mathbf{s}_{n_0}$ 是唯一确定的，

$$\mathbf{s}_0, \mathbf{s}_1, \cdots, \mathbf{s}_{n_0}, \mathbf{s}_{n_0+1}, \cdots, \mathbf{s}_{n_1-1}, \tag{5}$$

这些状态两两不同，而

$$(\mathbf{s}_{n_0}, \mathbf{s}_{n_0+1}, \cdots, \mathbf{s}_{n_1-1}) \tag{6}$$

就是状态图的一个圈，

$$\mathbf{s}_0, \mathbf{s}_1, \cdots, \mathbf{s}_{n_0-1} \tag{7}$$

都在这个圈的一个枝上．

证. 因n级移位寄存器一共有2^n个状态，所以状态序列(4)的前2^n+1项不能两两不同，因此总存在一个最小的正整数n_1使$\mathbf{s}_{n_1}$与足码比它小的一个状态$\mathbf{s}_{n_0}$相等. 根据n_1的最小性可知$\mathbf{s}_{n_0}$是唯一确定的，因而(5)中状态两两不同，由此推出(6)是一个圈而(7)在这个圈的一个支上.

n级移位寄存器的状态图的一个圈上的状态的个数，也即是构成这个圈的弧的个数，叫做这个圈的长，也叫这个圈的周期，例如，以f_1为反馈逻辑的4级移位寄存器的状态图有4个圈，3个的长是5，1个的长是1. 定理1中(6)这个圈的长是n_1-n_0.

从一个n级移位寄存器的任一状态$\mathbf{s}_0=(a_0, a_1, \cdots, a_{n-1})$出发，连续施行状态转移变换$T_f$得到一系列状态(4)，将(4)中每一状态$\mathbf{s}_k$的第一项$a_k$取出来，得到一个二元序列

$$a_0,\ a_1,\ a_2,\ \cdots,$$

这就是这个移位寄存器从初始状态$\mathbf{s}_0$出发产生的移位寄存器序列，根据定理1，存在一个非负整数n_0使

$$a_{n_0},\ a_{n_0+1},\ a_{n_0+2},\ \cdots \tag{8}$$

是个周期序列，周期是n_1-n_0，而$n_1-n_0\leqslant 2^n$. 从定理1立即推出，(8)的周期n_1-n_0与n_0的选取无关，这就证明了下面的系理.

系理 设

$$a_0,\ a_1,\ a_2,\ \cdots$$

是任一n级移位寄存器序列，那么总存在一个非负整数n_0使得

$$a_{n_0},\ a_{n_0+1},\ \cdots$$

是一个周期序列，它的周期$\leqslant 2^n$而且与n_0的选取无关.

值得注意的是，以f_1为反馈逻辑的移位寄存器的状态图由一些圈组成，而以g为反馈逻辑的移位寄存器的状态图除

了圈以外还有枝. 下面我们讨论“以什么样的开关函数为反馈逻辑的移位寄存器的状态图仅由一些圈组成”这一问题.

首先我们注意, 从一 n 级移位寄存器的状态图中任一顶点出发, 有一条且仅有一条弧以这个顶点为起点. 所以如果状态图中有两个圈有一公共顶点, 那么它们一定相重合. 由此立刻推出

定理 2 一个 n 级移位寄存器的状态图没有枝, 当且仅当它的状态图由一些两两没有公共顶点的圈组成.

再证明

定理 3 以 $f(x_1, x_2, \cdots, x_n)$ 为反馈逻辑的 n 级移位寄存器的状态图是没有枝的, 当且仅当它的状态转移变换 T_f 是从 $\mathbf{F}_{2^n}$ 到它自身之上的一个一一对应.

证. 当这个 n 级移位寄存器的状态图没有枝时, 根据定理 2, 它就由一些两两没有公共顶点的圈组成, 那么显然这个移位寄存器的状态转移变换 T_f 是个一一对应.

反之, 设 T_f 是个一一对应. 从任一状态 $\mathbf{s}_0$ 出发, 连续作用 T_f 可得一状态序列

$$\mathbf{s}_0,\ \mathbf{s}_1,\ \mathbf{s}_2,\ \cdots,$$

其中 $$\mathbf{s}_k = T_f(\mathbf{s}_{k-1}),\ k=1,\ 2,\ \cdots.$$

设 n_1 是最小的正整数使 $\mathbf{s}_{n_1}$ 与足码比它小的一个状态, 设为 $\mathbf{s}_{n_0}(n_0<n_1)$ 相等, 那么

$$\mathbf{s}_0,\ \mathbf{s}_1,\ \cdots,\ \mathbf{s}_{n_0},\ \cdots,\ \mathbf{s}_{n_1-1} \tag{9}$$

这 n_1 个状态两两相异. 如果 $n_0 \neq 0$, 那么

$$T_f(\mathbf{s}_{n_0-1}) = \mathbf{s}_{n_0},\ T_f(\mathbf{s}_{n_1-1}) = \mathbf{s}_{n_1} = \mathbf{s}_{n_0},$$

而 $$\mathbf{s}_{n_0-1} \neq \mathbf{s}_{n_1-1},$$

这与 T_f 是一一对应相矛盾. 所以一定有 $n_0=0$. 于是 (9) 就是状态图中的一个圈. 这证明了任一状态都在一个圈上. 因此这个移位寄存器的状态图没有枝.

定理4 以$f(x_1, x_2, \cdots, x_n)$为反馈逻辑的n级移位寄存器的状态图是没有枝的，当且仅当$f(x_1, x_2, \cdots, x_n)$可以表成

$$f(x_1, x_2, \cdots, x_n)=x_1+f_0(x_2, \cdots, x_n), \tag{10}$$

其中$f_0(x_2, \cdots, x_n)$是仅依赖于$x_2, \cdots, x_n$这$n-1$个变元的开关函数.

证. 先设$f(x_1, x_2, \cdots, x_n)$可以表成形状(10)，那么对任意状态$(a_1, a_2, \cdots, a_n)$,

$$\begin{aligned} f(\bar{a}_1, a_2, \cdots, a_n) &= (a_1+1)+f_0(a_2, \cdots, a_n) \\ &= 1+f(a_1, a_2, \cdots, a_n), \end{aligned}$$

于是对任意状态$(a_1, a_2, \cdots, a_n)$,

$$\begin{aligned} T_f(a_1, a_2, \cdots, a_n) &= (a_2, \cdots, a_n, f(a_1, a_2, \cdots, a_n)) \\ &\neq (a_2, \cdots, a_n, f(\bar{a}_1, a_2, \cdots, a_n)) \\ &= T_f(\bar{a}_1, a_2, \cdots, a_n) \end{aligned}$$

这表明T_f是从$\mathbf{F}_{2^n}$到它自身上的一一对应，因此根据定理3可知，以$f(x_1, x_2, \cdots, x_n)$为反馈逻辑的n级移位寄存器的状态图是没有枝的.

反之，设

$$f(x_1, x_2, \cdots, x_n)=x_1 f_1(x_2, \cdots, x_n)+f_0(x_2, \cdots, x_n),$$

而$f_1(x_2, \cdots, x_n)\neq 1$，那么有$(a_2, \cdots, a_n)\in\mathbf{F}_{2^{n-1}}$使

$$f(a_2, \cdots, a_n)=0.$$

于是对任意$a_1\in\mathbf{F}_2$,

$$f(a_1, a_2, \cdots, a_n)=f_0(a_2, \cdots, a_n)=f(\bar{a}_1, a_2, \cdots, a_n),$$

那么 $$T_f(a_1, a_2, \cdots, a_n)=T_f(\bar{a}_1, a_2, \cdots, a_n).$$

这就是说T_f不是一一对应. 仍根据定理3可知，以$f(x_1, x_2, \cdots, x_n)$为反馈逻辑的n级移位寄存器的状态图有枝.

我们说n元开关函数$f(x_1, x_2, \cdots, x_n)$是非异的，如果它可以表成形状(10)，而以非异n元开关函数$f(x_1, x_2, \cdots, x_n)$为反馈逻辑的n级移位寄存器就叫非异移位寄存器. 这样定

理 4 可以改述成

定理 5 n 级移位寄存器的状态图没有枝，当且仅当这个移位寄存器是非异的.

对于非异 n 级移位寄存器来说，从任一初始状态出发，它所产生的移位寄存器序列都是周期序列，其周期等于初始状态所在的圈的圈长，因此其周期一定 $\leqslant 2^n$. 由 n 级移位寄存器产生的周期 2^n 的移位寄存器序列，叫**最长 n 级移位寄存器序列**，简称 **M 序列**. 产生 M 序列的 n 级移位寄存器的状态图由一个圈长等于 2^n 的圈构成；因此从任一初始状态出发，这个移位寄存器所产生的移位寄存器序列都平移等价，因而都是周期 2^n 的 M 序列.

下面我们要证明：任给一个正整数 N，设 $2^{n-1}<N\leqslant 2^n$，那么总存在一个 n 级非线性移位寄存器，它的状态图中有一个长为 N 的圈，即它产生一个周期等于 N 的周期序列. 更进一步，还可以要求这个非线性移位寄存器是非异的.

首先引进一个符号和名词. 设

$$\mathbf{s}=(a_1,\ a_2,\ \cdots,\ a_n)\in\mathbf{F}_{2^n}.$$

令
$$\mathbf{s}^*=(\bar{a}_1,\ a_2,\ \cdots,\ a_n).$$

我们把 $\mathbf{s}$ 和 $\mathbf{s}^*$ 叫做**一对共轭状态**或**一对共轭顶点**.

我们先证明一条引理.

引理 1 设 $f(x_1,\ x_2,\ \cdots,\ x_n)$ 是个非异的 n 元开关函数. 令 $\mathbf{s}=(a_1,\ a_2,\ \cdots,\ a_n)$，$a_i=0$ 或 1. 置

$$f_{\mathbf{s}}(x_1,\ x_2,\ \cdots,\ x_n)=x_2^{a_2}x_3^{a_3}\cdots x_n^{a_n},$$

那么 $f+f_{\mathbf{s}}$ 也非异. 更进一步，如果 $\mathbf{s}$ 和 $\mathbf{s}^*$ 属于以 f 为反馈逻辑的 n 级移位寄存器的状态图 G_f 中不同的圈：

$$(\mathbf{s}_0=\mathbf{s},\ \mathbf{s}_1,\ \cdots,\ \mathbf{s}_{k_1}),\ (\mathbf{t}_0=\mathbf{s}^*,\ \mathbf{t}_1,\ \cdots,\ \mathbf{t}_{k_2}),\qquad(11)$$

那么以 $f+f_{\mathbf{s}}$ 为反馈逻辑的 n 级移位寄存器的状态图 $G_{f+f_{\mathbf{s}}}$ 可以将 G_f 的上述两个圈(11)合并成一个圈

$$(\mathbf{s}_0=\mathbf{s},\ \mathbf{t}_1,\ \cdots,\ \mathbf{t}_{k_2},\ \mathbf{t}_0=\mathbf{s}^*,\ \mathbf{s}_1,\ \cdots,\ \mathbf{s}_{k_1}),$$

并保持其余各圈不动而得到. 如果 $\mathbf{s}$ 和 $\mathbf{s}^*$ 属于 G_f 中同一个圈

$$(\mathbf{s}_0,\ \mathbf{s}_1,\ \cdots,\ \mathbf{s}_k),\tag{12}$$

而 $\mathbf{s}=\mathbf{s}_0,\ \mathbf{s}^*=\mathbf{s}_l\ (0<l\leqslant k)$,

那么 G_{f+f_s} 可以将 G_f 的上述一个圈(12)分成两个圈

$$(\mathbf{s}_0=\mathbf{s},\ \mathbf{s}_{l+1},\ \mathbf{s}_{l+2},\ \cdots,\ \mathbf{s}_k),\ (\mathbf{s}_l=\mathbf{s}^*,\ \mathbf{s}_1,\ \mathbf{s}_2,\ \cdots,\ \mathbf{s}_{l-1})$$

并保持其余各圈不动而得到.

证. $f+f_s$ 非异是很显然的. 将 $f+f_s$ 记作 f_1, 即 $f_1=f+f_s$. 如果 $(b_2,\ b_3,\ \cdots,\ b_n)\neq(a_2,\ \cdots,\ a_n)$, 那么

$$f_1(b_1,\ b_2,\ \cdots,\ b_n)=f(b_1,\ b_2,\ \cdots,\ b_n),$$

而

$$f_1(a_1,\ a_2,\ \cdots,\ a_n)=f(\bar{a}_1,\ a_2,\ \cdots,\ a_n),$$

$$f_1(\bar{a}_1,\ a_2,\ \cdots,\ a_n)=f(a_1,\ a_2,\ \cdots,\ a_n).$$

因此有 $T_{f_1}(\mathbf{t})=T_f(\mathbf{t})$, 对任一状态 $t\neq\mathbf{s},\ \mathbf{s}^*$,

而 $T_{f_1}(\mathbf{s})=T_f(\mathbf{s}^*),\ T_{f_1}(\mathbf{s}^*)=T_f(\mathbf{s})$.

由此即可推出本引理中所断言的 G_{f+f_s} 与 G_f 的关系.

注意, 实际上在 G_f 中交换 $\mathbf{s}$ 与 $\mathbf{s}^*$ 的后继就得到 G_{f+f_s}.

我们再证明

定理6 对任意给定的正整数 N, 设 $2^{n-1}<N\leqslant 2^n$, 那么总存在一个 n 级非异的非线性移位寄存器, 它产生一个周期等于 N 的移位寄存器序列.

证. 设

$$f(x)=1+c_1x+c_2x^2+\cdots+c_nx^n$$

是 $\mathbf{F}_2$ 上的 n 次本原多项式, 那么 $c_n=1$. 于是

$$f(x_1,\ x_2,\ \cdots,\ x_n)=c_nx_1+c_{n-1}x_2+\cdots+c_1x_n$$

是产生周期 2^n-1 的 m 序列的一个反馈逻辑. 设以 $f(x_1,\ x_2,\ \cdots,\ x_n)$ 为反馈逻辑 n 级线性移位寄存器产生的 m 序列是

$$a_0,\ a_1,\ a_2,\ \cdots.$$

令 $\mathbf{s}_k=(a_k, a_{k+1}, \cdots, a_{k+n-1}), k=0, 1, 2, \cdots, 2^n-2,$
那么
$$\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \cdots, \mathbf{s}_{2^n-2}$$
就是 2^n-1 个两两不同的非零状态，它们组成 G_f 的一个周期 2^n-1 的圈：
$$(\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \cdots, \mathbf{s}_{2^n-2}). \tag{13}$$
G_f 还有一个周期等于 1 的圈，它由全 0 状态
$$\mathbf{0}=(\underbrace{0, 0, \cdots, 0}_{n\text{个}0})$$
构成.

当 $N=2^n-1$ 时，本定理显然成立.

再考察 $N=2^n$ 的情形. 我们知道
$$(1, \underbrace{0, \cdots, 0}_{n-1\text{个}0})$$
是一个非零状态，因此一定在圈(13)中出现. 设
$$\mathbf{s}_{k_0}=(1, 0, \cdots, 0), 0\leqslant k_0\leqslant 2^n-2.$$
因 $\mathbf{s}_{k_0}$ 和 $\mathbf{0}$ 是一对共轭状态，于是从引理 1 就可推出，以
$$\begin{aligned} &f(x_1, x_2, \cdots, x_n)+\bar{x}_2\bar{x}_3\cdots\bar{x}_n \\ &\quad=c_nx_1+c_{n-1}x_2+\cdots+c_1x_n+\bar{x}_2\bar{x}_3\cdots\bar{x}_n \end{aligned} \tag{14}$$
为反馈逻辑的 n 级非线性移位寄存器的状态图就是一个周期等于 2^n 的圈
$$(\mathbf{s}_0, \mathbf{s}_1, \cdots, \mathbf{s}_{k_0}, \mathbf{0}, \mathbf{s}_{k_0+1}, \mathbf{s}_{k_0+2}, \cdots, \mathbf{s}_{2^n-2}).$$
因此它产生一个周期等于 2^n 的 M 序列. 又因 $c_n=1$, 所以(14)是非异的. 这证明了本定理对 $N=2^n$ 成立.

以下设 $2^{n-1}<N<2^n-1$. 如果能在 G_f 的圈 (13) 中找到一对相距 N 的共轭状态
$$\mathbf{s}_{k_0}, \mathbf{s}_{k_0+N}=\mathbf{s}_{k_0}^*$$
那么根据引理 1, 以
$$f(x_1, x_2, \cdots, x_n)+x_2^{a_{k_0+1}}x_3^{a_{k_0+2}}\cdots x_n^{a_{k_0+(n-1)}}$$

为反馈逻辑的非异的非线性移位寄存器就有一个长为 N 的圈:

$$(\mathbf{s}_{k_0+1},\ \mathbf{s}_{k_0+2},\ \cdots,\ \mathbf{s}_{k_0+N}).$$

因此它从初始状态

$$\mathbf{s}_{k_0+1}=(a_{k_0+1},\ a_{k_0+2},\ \cdots,\ a_{k_0+n})$$

出发就产生一个周期等于 N 的移位寄存器序列. 于是问题化为证明有 $\mathbf{s}_{k_0}(0\leqslant k\leqslant 2^n-2)$ 存在,具有性质:

$$\mathbf{s}_{k_0}^*=\mathbf{s}_{k_0+N}. \tag{15}$$

令

$$T_f=\begin{pmatrix} 0 & & & & -c_n \\ 1 & 0 & & & -c_{n-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -c_2 \\ & & & 1 & -c_1 \end{pmatrix}.$$

那么

$$\mathbf{s}_{k_0+N}=\mathbf{s}_{k_0}T_f^N.$$

于是条件(15)就成为

$$\mathbf{s}_{k_0}+(1,\ 0,\ \cdots,\ 0)=\mathbf{s}_{k_0}T_f^N,$$

即

$$\mathbf{s}_{k_0}(I+T_f^N)=(1,\ 0,\ \cdots,\ 0). \tag{16}$$

我们来证明 $|I+T_f^N|\neq 0$. 如果 $|I+T_f^N|=0$, 那么齐次线性方程组

$$(I+T_f^N)'(x_1,\ x_2,\ \cdots,\ x_n)'=\mathbf{0}'$$

有非零解 $(b_1,\ b_2,\ \cdots,\ b_n)'$. 于是

$$(b_1,\ b_2,\ \cdots,\ b_n)(I+T_f^N)=(0,\ 0,\ \cdots,\ 0).$$

因此

$$(b_1,\ b_2,\ \cdots,\ b_n)T_f^N=(b_1,\ b_2,\ \cdots,\ b_n). \tag{17}$$

将 $(b_1,\ b_2,\ \cdots,\ b_n)$ 看作一非零状态, 因 2^n-1 个非零状态组成一个周期 2^n-1 的圈, 所以从 (17) 推出 $2^n-1|N$. 但 $N<2^n-1$, 这是一个矛盾. 因此 $|I+T_f^N|\neq 0$, 即 $I+T_f^N$ 是个非异矩阵,那么从(16)式可解出

$$\mathbf{s}_{k_0}=(1,\ 0,\ \cdots,\ 0)(I+T_f^N)^{-1}.$$

这就证明了本定理当 $2^{n-1}<N<2^n-1$ 时也成立.

值得注意的是，定理6的证明是构造性的. 特别对于 $N=2^n$ 这一情形，定理6的证明还给出了构造产生周期 2^n 的 M 序列的反馈逻辑的一个方法. 用这个方法一共可以得到 $\varphi(2^n-1)/n$ 个产生周期 2^n 的 M 序列的反馈逻辑，但 de Bruijn, N. G. 曾经证明*，一共有 $2^{2^{n-1}-n}$ 个两两平移不等价的周期等于 2^n 的 M 序列，即一共有 $2^{2^{n-1}-n}$ 个两两相异的产生周期等于 2^n 的 M 序列的反馈逻辑. 当 n 大时，$\varphi(2^n-1)/n$ 较 $2^{2^{n-1}-n}$ 要小得多. $n\leqslant 6$ 时，下面列出了这两个数的值:

表 4

n	1	2	3	4	5	6
$\varphi(2^n-1)/n$	1	1	2	2	6	6
$2^{2^{n-1}}-n$	1	1	2	16	2,048	67,108,864

如何将产生 M 序列的反馈逻辑都具体求出来，是一个有意义的问题.

对于 $2^{n-1}<N<2^n-1$ 的情形，定理6的证明也给出了构造产生周期等于 N 的移位寄存器序列的方法. 当选定一个 n 次本原多项式 $f(x)$ 之后，问题是要求

$$\mathbf{s}_{k_0}=(1,\ 0,\ \cdots,\ 0)(I+T_f^N)^{-1}.$$

因此关键在于计算 $(I+T_f^N)^{-1}$. 下面我们介绍一个计算 $(I+T_f^N)^{-1}$ 的算法. 根据第二章 §5 定理4(即 Cayley-Hamilton 定理)，T_f 适合它的特征多项式

$$\tilde{f}(x)=|xI-T_f|=x^n+c_1x^{n-1}+\cdots+c_n.$$

因 $\tilde{f}(x)$ 是与 $f(x)$ 互反的多项式，所以 $\tilde{f}(x)$ 也是 n 次本原多

* de Bruijn, N. G., A Combinatorial Problem, Koninklijke Nederlands Akademie von Wetenschappen, Proceedings, 49(1946), 758—764.

项式. 将 N 表成二进位数

$$N=l_0 2^0+l_1 2^1+l_2 2^2+\cdots+l_m 2^m,$$

其中 $l_i=0$ 或 1, 而 $l_m=1$. 依序计算

$$(x^{2^0})_{(x)},\ (x^{2^1})_{\tilde{f}(x)},\ (x^{2^2})_{\tilde{f}(x)},\ \cdots,\ (x^{2^m})_{\tilde{f}(x)}. \tag{18}$$

再令 $$h(x)=1+[(x^{2^0})_{\tilde{f}(x)}]^{l_0}[(2^{2^1})_{\tilde{f}(x)}]^{l_1}[(x^{2^2})_{\tilde{f}(x)}]^{l_2}\cdots \cdot[(x^{2^m})_{\tilde{f}(x)}]^{l_m}.$$

因 $\tilde{f}(x)$ 不可约, 而 $\partial^0 h(x)<n=\partial^0 f(x)$, 所以 $\tilde{f}(x)$ 和 $h(x)$ 互素,那么用辗转相除法和第一章§2定理2的证明方法可求得非零多项式 $a(x)$ 和 $b(x)$, 而 $\partial^0 a(x)<\partial^0\tilde{f}(x)$, $\partial^0 b(x)<\partial^0 h(x)$ 使

$$a(x)h(x)+b(x)\tilde{f}(x)=1.$$

将 T_f 代入上式就得到

$$a(T_f)h(T_f)=I,$$

因此 $$a(T_f)=h(T_f)^{-1}=(I+T_f^N)^{-1}.$$

我们再指出在计算(18)中的一系列多项式时, 可以按照下面的算法进行:

(1) 先计算

$$(x^0)_{\tilde{f}(x)},\ (x^2)_{\tilde{f}(x)},\ (x^{2\cdot 2})_{\tilde{f}(x)},\ \cdots,\ (x^{2(n-1)})_{\tilde{f}(x)}.$$

设 $$(x^{2j})_{\tilde{f}(x)}=\sum_{i=0}^{n-1}a_{ij}x^i,\ j=0,\ 1,\ 2,\ \cdots,\ n-1,$$

其中 $a_{ij}=0$ 或 1. 我们就得到一个 $n\times n$ 矩阵

$$A=(a_{ij})_{0\leqslant i,j\leqslant n-1}.$$

(2) 再计算

$$(x^{2^0})_{\tilde{f}(x)},\ (x^{2^1})_{\tilde{f}(x)},\ (x^{2^2})_{\tilde{f}(x)},\ \cdots,\ (x^{2^m})_{\tilde{f}(x)}.$$

注意, 当 $2^i<2(n-1)$ 时, $2^i=2(2^{i-1})$ 而 $2^{i-1}<n-1$, 因此

$$(x^{2^i})_{\tilde{f}(x)}$$

在第(1)步已经算出. 又如果已经算出

$$(x^{2^i})_{\tilde{f}(x)} = \sum_{j=0}^{n-1} b_j x^j,$$

那么 $$(x^{2^{i+1}})_{\tilde{f}(x)} = ([(x^{2^i})_{\tilde{f}(x)}]^2)_{\tilde{f}(x)} = \left(\left[\sum_{j=0}^{n-1} b_j x^j\right]^2\right)_{\tilde{f}(x)}$$

$$= \left(\sum_{j=0}^{n-1} b_j x^{2j}\right)_{\tilde{f}(x)} = \sum_{j=0}^{n-1} b_j \sum_{i=0}^{n-1} a_{ij} x^i$$

$$= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} a_{ij} b_j\right) x^i.$$

因此，如果令 $$(x^{2^{i+1}})_{\tilde{f}(x)} = \sum_{j=0}^{n-1} b'_j x^j,$$

那么

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ \vdots \\ b'_{n-1} \end{pmatrix} = A \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{pmatrix}. \tag{19}$$

当 $(x^{2^i})_{\tilde{f}(x)}$ 已经算出，那么用公式(19)来计算 $(x^{2^{i+1}})_{\tilde{f}(x)}$ 是很方便的.

在[20]的附录三里，有 Baumert, L. D. 编的一个产生周期等于 $N \leqslant 2047$ 的非线性移位寄存器的反馈逻辑的表.

现在我们来讨论，怎样利用定理 6 来设计产生给定的一个伪随机序列的硬件这一问题. 设

$$b_0, b_1, b_2, \cdots \tag{20}$$

是一个周期等于 N 的二元周期序列(特别，伪随机序列). 设 $2^{n-1} < N \leqslant 2^n$. 先利用定理 6, 造一个 n 级非线性移位寄存器，它能产生一个周期 N 的移位寄存器序列

$$a_0, a_1, a_2, \cdots,$$

设这个 n 级非线性移位寄存器的反馈逻辑是 $f(x_1, x_2, \cdots, x_n)$, 再构造一个 n 元开关函数 $g(x_1, x_2, \cdots, x_n)$, 具有性质

$$g(a_k, a_{k+1}, \cdots, a_{k+(n-1)}) = b_k, \quad 0 \leqslant k \leqslant N-1. \tag{21}$$

考察下面的框图：

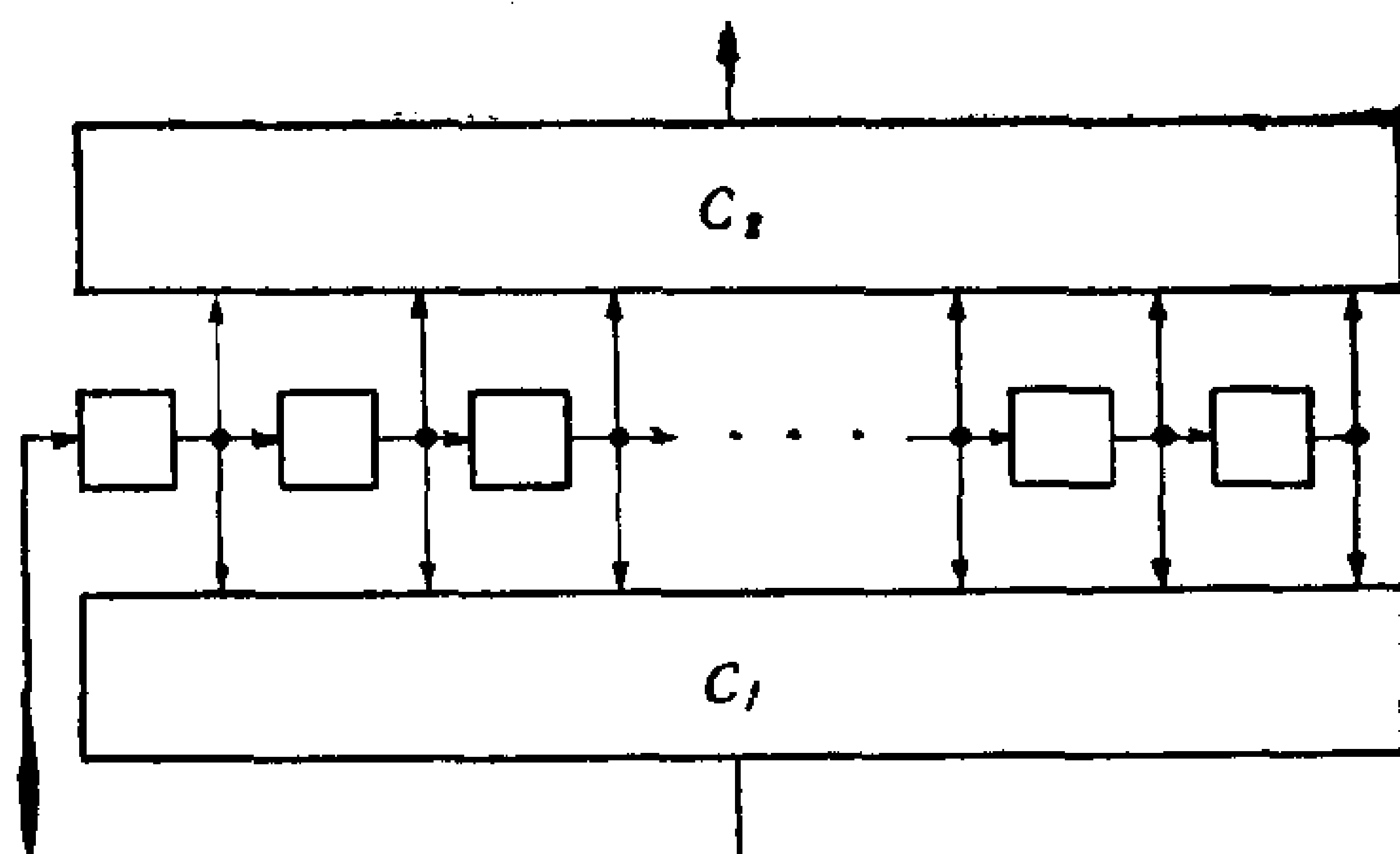


图 4

中间一排有 n 个小方框，代表 n 个寄存器；上面的长方框代表一个有 n 个输入端和 1 个输出端的开关线路，它实现 n 元开关函数 $g(x_1, x_2, \cdots, x_n)$，叫做外部电部；而下面的长方框也代表一个有 n 个输入端和 1 个输出端的开关线路，它实现 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$. 将它的 n 个寄存器从右往左依序置以 $a_0, a_1, a_2, \cdots, a_{n-1}$，那么不断地加移位脉冲，开关线路 C_g 的输出就是事先给定的周期等于 N 的二元序列(20)。

至于怎样求一个 n 元开关函数 $g(x_1, x_2, \cdots, x_n)$ 具有性质(21)请读者参考有关开关线路的书.

我们再介绍一个用一个非线性移位寄存器直接产生事先给定的周期等于 N 的二元序列 (20) 的方法. 第一步是求一个最小的具有以下性质的正整数 n: 对任意 $i_1, i_2(0\leqslant i_1<i_2\leqslant N-1)$，如果 $(b_{i_1}, b_{i_1+1}, \cdots, b_{i_1+(n-1)}) = (b_{i_2}, b_{i_2+1}, \cdots, b_{i_2+(n-1)})$，那么一定有 $b_{i_1+n}=b_{i_2+n}$. 这可以依次检查 1, 2, ⋯ 看那一个正整数最先具有这个性质，而最先具有上述性质的正整数一定是最小的具有上述性质的正整数. 第二步是构造一个 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 具有性质

$$f(b_k, b_{k+1}, \cdots, b_{k+(n-1)})=b_{k+n},\ 0\leqslant k\leqslant N-1.$$

这时，以$f(x_1, x_2, \cdots, x_n)$为反馈逻辑的n级移位寄存器从初始状态$(b_0, b_1, \cdots, b_{n-1})$出发就产生事先给定的周期等于$N$的二元序列(20). 这种产生(20)的方法叫做直接方法，而前面介绍的方法则叫做间接方法.

最后我们指出，目前关于非线性移位寄存器的结果还很初步，这是一个很值得探讨的对象. 对它有兴趣的读者可参考[1].

§10 自律线性时序线路

前面我们讨论了反馈移位寄存器. 有时我们常将移位寄存器用另外一些方式联接起来；下面这几个框图里的线路就是例子：

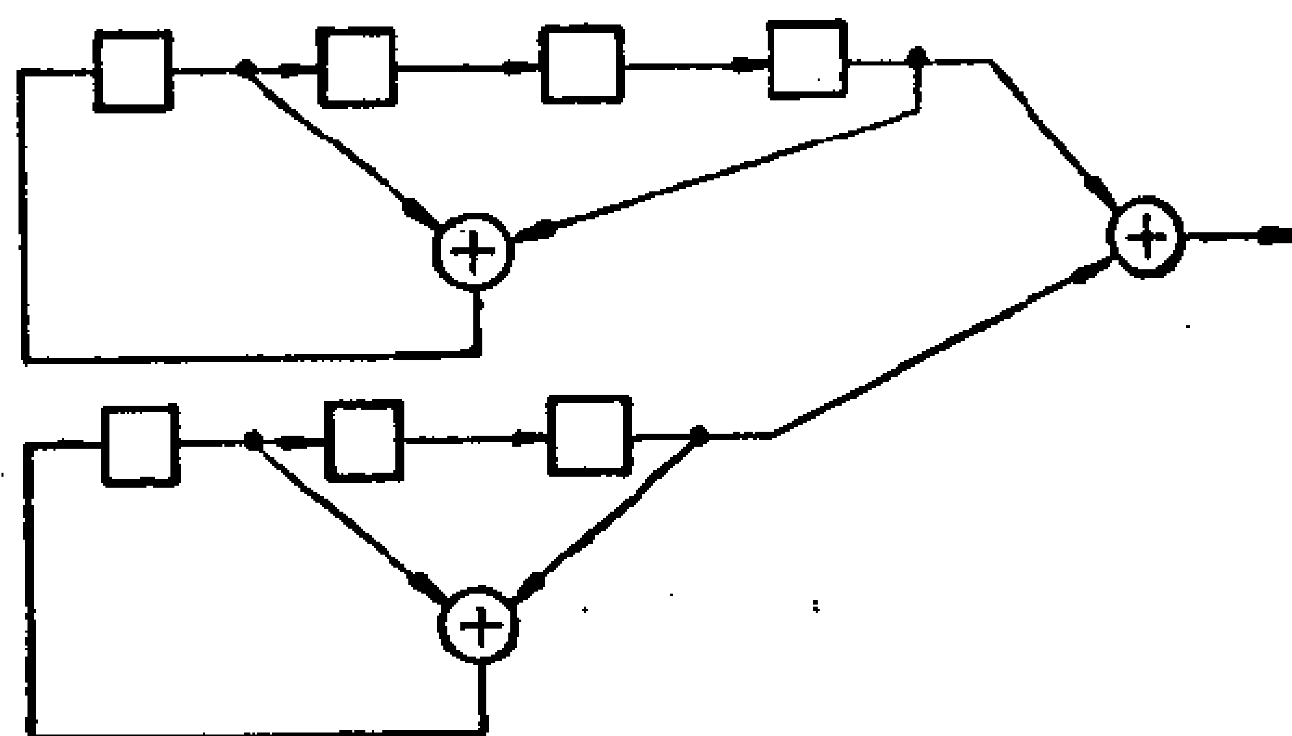


图 1

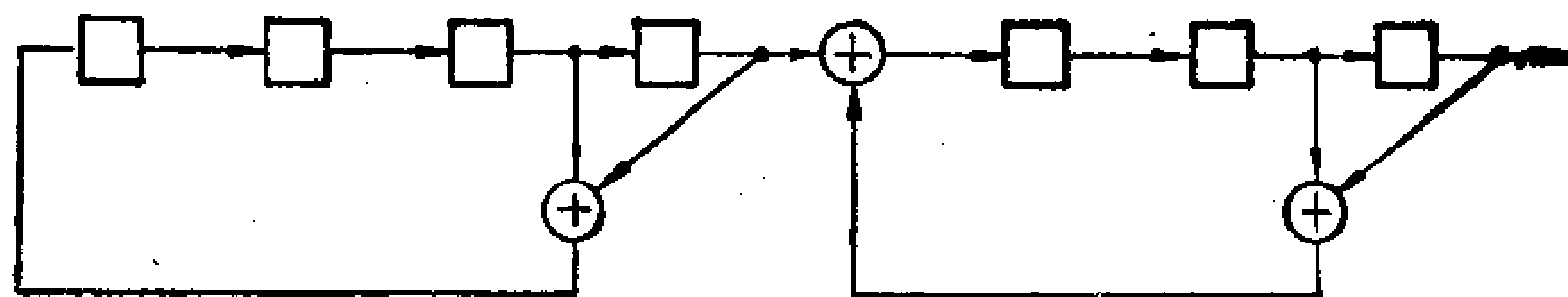


图 2

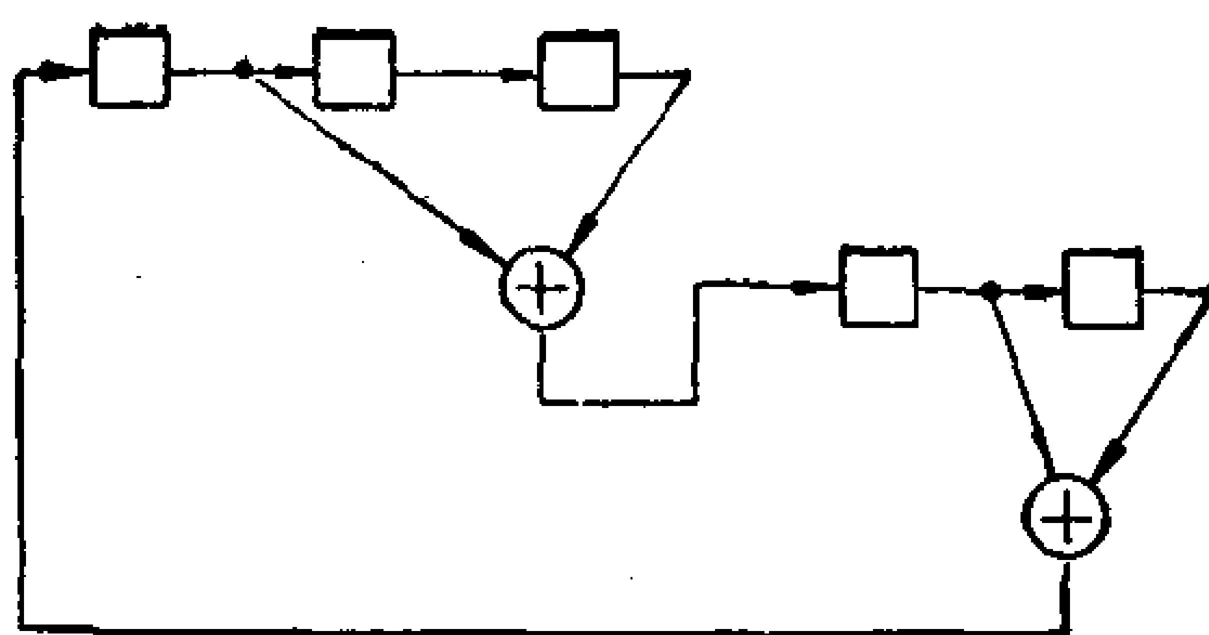


图 3

特别，图1是将两个线性反馈移位寄存器并联而得的线路；图2是将两个线性反馈移位寄存器串联而得的线路；图3是将两个线性移位寄存器经互馈联接而得的线路．这三个线路和线性反馈移位寄存器一样也都是由延迟元件(即寄存器)和线性开关元件(即模2加法器)组成；但不同的是，它们都有多个延迟元件，这些延迟元件的输入是开关元件的输出．它们都是所谓的自律线性时序线路．作为前面讨论的(反馈)移位寄存器的推广，在这一节里我们来讨论自律时序线路，特别是自律线性时序线路．我们先讨论没有输出的自律线性时序线路，然后再讨论一般的，即有输出自律线性时序线路，最后再讨论它的一些应用．

下面是没有输出的自律时序线路的框图．

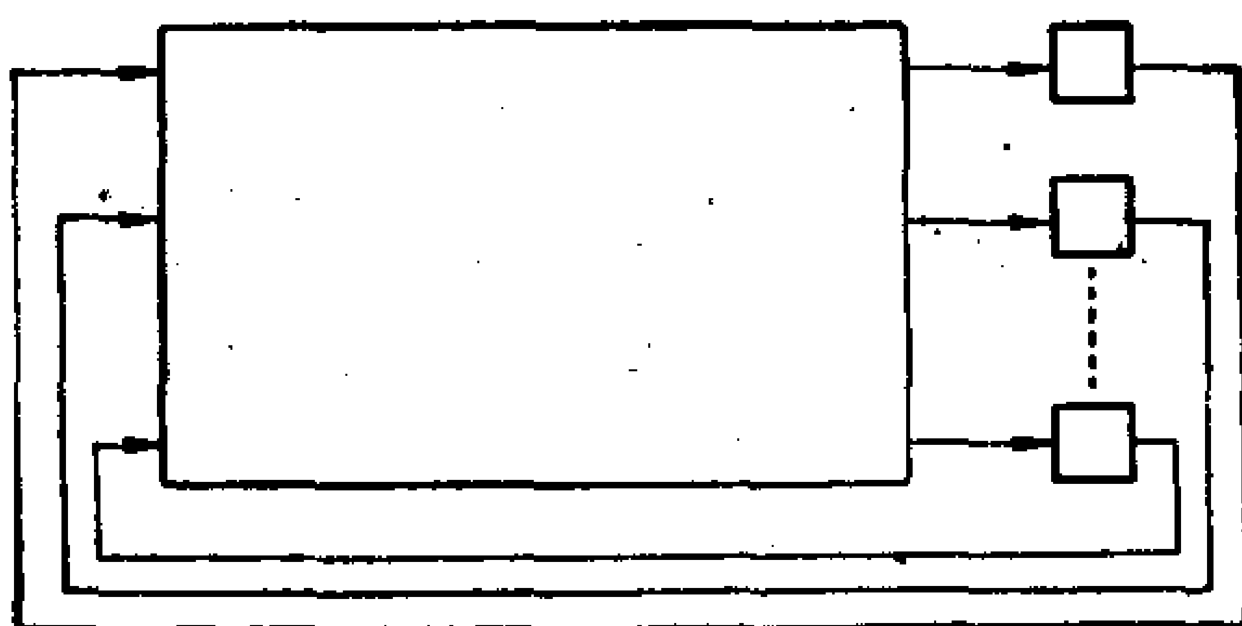


图 4

上图中小方框代表寄存器，它在任一时刻的输出都等于前一时刻它的输入(即它的内容)；左面的大长方框代表一个开关线路，叫做这个自律时序线路的反馈开关线路．假定有 n 个寄

存器，从上到下依序叫做第1个、第2个、…、第n个寄存器。那么右面的反馈开关线路就是有n个输入端和n个输出端的开关线路。我们约定寄存器的输入(即内容)和输出以及反馈开关线路的输入和输出都在q个元素的有限域$\mathbf{F}_q$中取值，而q是一个素数的幂。再假定时间t是离散的，即t依序取0, 1, 2, …诸值。设在时刻$t(t=0, 1, 2, \cdots)$，上述自律时序线路的n个寄存器的内容自上到下依序是$s_1(t), s_2(t), \cdots, s_n(t)$，它们都是$\mathbf{F}_q$中的元素，我们就说这个自律时序线路在时刻$t$的状态是

$$\mathbf{s}(t)=(s_1(t),\ s_2(t),\ \cdots,\ s_n(t)) \tag{1}$$

因此$\mathbf{s}(t)$可看作$\mathbf{F}_q$上n维行向量空间$V_n(\mathbf{F}_q)$中的向量。注意，在时刻$t+1$，n个寄存器的输出$s_1(t), s_2(t), \cdots, s_n(t)$即是反馈开关线路$n$个输入端的输入。那么在时刻$t+1$，反馈开关线路$n$个输出端的输出可表作

$$f_i(s_1(t),\ s_2(t),\ \cdots,\ s_n(t)),\ i=1,\ 2,\ \cdots,\ n \tag{2}$$

这里$f_1, f_2, \cdots, f_n$都是在$\mathbf{F}_q$中取值的n元(开关)函数，n个变元也都在$\mathbf{F}_q$中取值。当然，$f_1, f_2, \cdots, f_n$由反馈开关线路唯一确定。再注意，在时刻$t+1$，(2)又是n个寄存器的输入。因此在时刻$t+1$，n个寄存器的内容$s_i(t+1)$ $(i=1, 2, \cdots, n)$是

$$s_i(t+1)=f_i(s_1(t),\ s_2(t),\ \cdots,\ s_n(t)),\ i=1,\ 2,\ \cdots,\ n. \tag{3}$$

例如，一个以$1+c_1x+c_2x^2+\cdots+c_nx^n$为联接多项式的$n$级线性反馈移位寄存器，如果不考虑它的输出，就可以看作是一个自律时序线路；这只要将它的n个寄存器从右往左依序叫做第1个，第2个，…，第n个寄存器*，并令

$$f_n(x_1,\ x_2,\ \cdots,\ x_n)=-c_nx_1-c_{n-1}x_2-\cdots-c_2x_{n-1}-c_1x_n$$

* 注意，以前我们把n级反馈移位寄存器的n个寄存器从左往右依序叫做第1级，第2级，…，第n级寄存器。

$$f_i(x_1, x_2, \cdots, x_n) = x_{i+1}, \quad i=1, 2, \cdots, n-1$$

就行了. 类似地也可以把 n 级非线性反馈移位寄存器看作自律时序线路.

当(2)中的 $f_1, f_2, \cdots, f_n$ 都是 n 元线性齐次函数时, 即

$$f_j(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{n} a_{ij}x_i, \quad a_{ij} \in \mathbf{F}_q, \quad j=1, 2, \cdots, n,$$

上述自律时序线路就叫自律线性时序线路. 令

$$A = (a_{ij})_{1 \leqslant i, j \leqslant n},$$

那么(3)式可改写作

$$\mathbf{s}(t+1) = \mathbf{s}(t)A. \tag{4}$$

于是 A 叫做这个自律线性时序线路的状态转移矩阵, 它由这个自律线性时序线路唯一确定. 以 A 为状态转移矩阵的自律线性时序线路的反馈开关线路记作 C_A, 我们还往往在它的框图里的反馈开关线路的长方框中标记上 A.

在前一段里已经说过, 可以把 n 级反馈移位寄存器看作自律时序线路, 特别可以把 n 级线性反馈移位寄存器看作自律线性时序线路. 如果一个 n 级线性反馈移位寄存器的联接多项式是

$$f(x) = 1 + c_1x + c_2x^2 + \cdots + c_nx^n,$$

那么它的变换矩阵(也叫它的状态转移矩阵)

$$\begin{pmatrix} 0 & & & & -c_n \\ 1 & 0 & & & -c_{n-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -c_2 \\ & & & 1 & -c_1 \end{pmatrix}$$

也就是将它看作自律线性时序线路时的状态转移矩阵.

我们来定义以 A 为状态转移矩阵的自律线性时序线路的状态图, 记作 G_A. G_A 是一个有 q^n 个顶点和 q^n 条弧的有向

图. 它的顶点集是

$$V_n(\mathbf{F}_q)=\{(a_1, a_2, \cdots, a_n)\,|\,a_1, a_2, \cdots, a_n\in\mathbf{F}_q\},$$

每个顶点代表一个状态. 设 $(a_1, a_2, \cdots, a_n)$ 是 G_A 的一个顶点,并设

$$(b_1, b_2, \cdots, b_n)=(a_1, a_2, \cdots, a_n)A,$$

那么 G_A 就有一条以 $(a_1, a_2, \cdots, a_n)$ 为起点而以 $(b_1, b_2, \cdots, b_n)$ 为终点的弧. 这样就得到 G_A 的 q^n 条弧. 于是 G_A 的每个顶点都是唯一的一条弧的起点. G_A 的每条弧都表明它的起点所代表的状态怎样按状态转移矩阵 A 转移. 显然 G_A 由 A 完全确定. 我们也往往把 G_A 叫做 A 的图.

为了讨论自律线性时序线路的状态图, 引进有向图的一些概念是有好处的.

定义 1 一个有向图 G 被认为是由两个有限集合 V 和 A 组成,而 A 是

$$V^2=\{(x, y)\,|\,x, y\in V\}$$

的一个子集. 我们把 V 中元素叫做 G 的顶点,而 V 叫做 G 的顶点集, 把 A 中元素叫做 G 的弧, 而 A 叫做 G 的弧集. 为明确起见, 有时我们把以 V 为顶点集而以 A 为弧集的有向图 G 记作 $G(V, A)$. 如果 $x, y\in V$ 而 $(x, y)\in A$, (x, y) 就叫以 x 为起点而以 y 为终点的弧, x 叫 y 的一个先导,而 y 叫 x 的一个后继.

定义 2 设 $G(V, A)$ 和 $G'(V', A')$ 是两个有向图. 如果存在一个从 V 到 V' 之上的一一对应 σ, 使得对 G 中任意二顶点 x 和 y: $(x, y)\in A$, 当且仅当 $(\sigma(x), \sigma(y))\in A'$, 我们就说 G 和 G' 同构,而 σ 就叫从 G 到 G' 的一个同构.

定理 1 设 A 和 B 是相似的 $n\times n$ 矩阵,那么它们的图 G_A 和 G_B 一定同构.

证. 设 $$B=P^{-1}AP,$$

而 P 是 $\mathbf{F}_q$ 上的 $n\times n$ 可逆矩阵. 建立一个从 G_A 的顶点集到 G_B 的顶点集上的一一对应.

$$\sigma:(a_1,\ a_2,\ \cdots,\ a_n)\to(a_1,\ a_2,\ \cdots,\ a_n)P,$$

那么 $$\sigma((a_1,\ a_2,\ \cdots,\ a_n)A)=(a_1,\ a_2,\ \cdots,\ a_n)AP$$
$$=((a_1,\ a_2,\ \cdots,\ a_n)P)B.$$

显然 G_B 中有一条以 $(a_1,\ a_2,\ \cdots,\ a_n)P$ 为起点而以 $((a_1,\ a_2,\ \cdots,\ a_n)P)\ B$ 为终点的弧. 因此 σ 是从 G_A 到 G_B 的一个同构.

容易举例说明定理1的逆并不成立，请读者自己举一个例.

根据定理1, 要研究 A 的图 G_A, 只要研究 A 在相似变换下的标准形的图就行了. 我们有

定理 2 以 $\mathbf{F}_q$ 上的 $n\times n$ 矩阵 A 为状态转移矩阵的自律线性时序线路的状态图, 即 A 的图, 同构于由若干个没有输出的线性(反馈)移位寄存器并列而成的自律线性时序线路的状态图.

证. 设 A 的初等因子组是

$$p_i(x)^{e_{ij}},\ j=1,\ 2,\ \cdots,\ r_i,\ i=1,\ 2,\ \cdots,\ s,$$

其中 $p_1(x),\ p_2(x),\ \cdots,\ p_s(x)$ 是 s 个两两不同的不可约多项式, 而 e_{ij} 是正整数具有性质:

$$e_{i1}\geqslant e_{i2}\geqslant\cdots\geqslant e_{ir_i}>0,\ i=1,\ 2,\ \cdots,\ s,$$

那么 $$\sum_{i=1}^{s}\left(\sum_{j=1}^{r_i}e_{ij}\right)\cdot\partial^0 p_i(x)=n.$$

令 $$n_{ij}=e_{ij}\cdot\partial^0 p_i(x),$$

写

$$p_i(x)^{e_{ij}}=x^{n_{ij}}+c_1^{(i,j)}x^{n_{ij}-1}+c_2^{(i,j)}x^{n_{ij}-2}+\cdots+c_{n_{ij}}^{(i,j)},\ c_k^{(i,j)}\in\mathbf{F}_q.$$

再令

$$M(p_i(x)^{e_{ij}})=\begin{pmatrix} 0 & & & & -c_{n_{ij}}^{(i,j)} \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \\ & & \ddots & 0 & -c_2^{(i,j)} \\ & & & 1 & -c_1^{(i,j)} \end{pmatrix},$$

并将 $M(p_i(x)^{e_{ij}})$ 简记作 M_{ij}. 那么 A 相似于有理标准形

$$B=\begin{pmatrix} M_{11} & & & & & & & & & & & \\ & M_{12} & & & & & & & & & & \\ & & \ddots & & & & & & & & & \\ & & & M_{1r_1} & & & & & & & & \\ & & & & M_{21} & & & & & & & \\ & & & & & M_{22} & & & & & & \\ & & & & & & \ddots & & & & & \\ & & & & & & & M_{2r_2} & & & & \\ & & & & & & & & \ddots & & & \\ & & & & & & & & & M_{s1} & & \\ & & & & & & & & & & M_{s2} & \\ & & & & & & & & & & & \ddots \\ & & & & & & & & & & & & M_{sr_s} \end{pmatrix} \qquad (5)$$

令
$$f_{ij}(x)=x^{n_{ij}}p_i(1/x)^{e_{ij}},$$
那么以 $f_{ij}(x)$ 为联接多项式的 n_{ij} 级线性移位寄存器的状态转移矩阵就是 M_{ij}, $i=1, 2, \cdots, s$, $j=1, 2, \cdots, r_i$. 因此将这 $r_1+r_2+\cdots+r_s$ 个线性移位寄存器并列，并不考虑它们的输出，所得到的自律线性时序线路的状态转移矩阵就是 B. 根据定理 1，这样所得到的自律线性时序线路的状态图与 A 的图同构.

下面我们先分别研究非异矩阵和幂零矩阵的图，然后再利用这两个情形的结果去讨论一般情形.

先研究 A 是非异矩阵的情形．首先，我们有

定理 3 非异矩阵的图由一些圈组成．

证．对任一 $n\times n$ 矩阵 A，G_A 中任一顶点 $(a_1, a_2, \cdots, a_n)$ 都是 G_A 中唯一的一条弧的起点，这条弧的终点是 $(a_1, a_2, \cdots, a_n)A$．当 A 是非异矩阵时，$(a_1, a_2, \cdots, a_n)$ 又是 G_A 中唯一的一条弧的终点，这条弧的起点是 $(a_1, a_2, \cdots, a_n)A^{-1}$．由这两点就可以推出 G_A 由一些圈组成．

和在 § 3 中对非退化的线性移位寄存器的状态图所做的一样，也可以用圈元来形式地表示非异矩阵的图．设非异矩阵 A 的图 G_A 由 n_1 个长为 1 的圈，n_2 个长为 2 的圈，…，n_i 个长为 i 的圈，… 组成，那么形式地记

$$\Sigma_A = n_1[1] + n_2[2] + \cdots + n_i[i] + \cdots,$$

其中 [1]，[2]，… 是些形式符号．我们把 Σ_A 叫做 G_A 的圈元．注意，Σ_A 是个有限和，即只有有限个 n_i 不等于 0．

现在利用定理 2 来研究非异矩阵 A 的图 G_A 的圈元．仍采用定理 2 的证明中的记号．我们知道 $G_{M_{ij}}$ 是以 $f_{ij}(x) = x^{n_{ij}}p_i(1/x)^{e_{ij}}$ 为联接多项式的线性移位寄存器的状态图．因 $f_{ij}(x) = \widetilde{p}_i(x)^{e_{ij}}$，而 $\widetilde{p}_i(x)$ 是 $p_i(x)$ 的互反多项式，因此 $\widetilde{p}_i(x)$ 也是不可约多项式，所以 $G_{M_{ij}}$ 的圈元 $\Sigma_{M_{ij}}$ 可以从 § 3 定理 4′ 得到．为了从 $r_1 + r_2 + \cdots + r_s$ 个 $G_{M_{ij}}$ 的圈元 $\Sigma_{M_{ij}}$ 得到 G_A 的圈元 Σ_A，我们先证明

引理 1 设 A 是 $n\times n$ 非异矩阵，并假定

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

其中 A_1 和 A_2 分别是 $n_1\times n_1$ 和 $n_2\times n_2$ 矩阵，而 $n_1 + n_2 = n$．再设 $\mathbf{s}_k \in V_{n_k}(\mathbf{F}_q)$，而 $\mathbf{s}_k$ 是 G_{A_k} 的一个长为 l_k 的圈上的顶点 $(k=1, 2)$．那么 $(\mathbf{s}_1, \mathbf{s}_2)$ 就是 G_A 的一个长为 $[l_1, l_2]$ 的圈上的顶点．

证. $\mathbf{s}_k$ 是 G_{A_k} 的一个长为 l_k 的圈上的顶点，当且仅当 l_k 是最小正整数使得

$$\mathbf{s}_k A_k^{l_k} = \mathbf{s}_k.$$

设 $(\mathbf{s}_1, \mathbf{s}_2)$ 是 G_A 的一个长为 l 的圈上的顶点，并设 $l' = [l_1, l_2]$. 那么显然有

$$(\mathbf{s}_1, \mathbf{s}_2)A^{l'} = (\mathbf{s}_1 A_1^{l'}, \mathbf{s}_2 A_2^{l'}) = (\mathbf{s}_1, \mathbf{s}_2),$$

因此 $l | l'$. 又从

$$(\mathbf{s}_1, \mathbf{s}_2)A^l = (\mathbf{s}_1, \mathbf{s}_2)$$

推出
$$\mathbf{s}_1 A_1^{l_1} = \mathbf{s}_1, \ \mathbf{s}_2 A_2^{l_2} = \mathbf{s}_2$$

因此 $l_1 | l$, $l_2 | l$, 于是 $l' | l$. 所以 $l = l'$.

从引理 1 立刻推出，如果 $(\mathbf{s}_{11}, \mathbf{s}_{12}, \cdots, \mathbf{s}_{1l_1})$ 是 G_{A_1} 的一个长为 l_1 的圈，而 $(\mathbf{s}_{21}, \mathbf{s}_{22}, \cdots, \mathbf{s}_{2l_2})$ 是 G_{A_2} 的一个长为 l_2 的圈，那么 G_A 的下面这 $l_1 l_2$ 个顶点

$$(\mathbf{s}_{1i}, \mathbf{s}_{2j}),\ 1 \leqslant i \leqslant l_1,\ 1 \leqslant j \leqslant l_2$$

就是 G_A 的 (l_1, l_2) 个长为 $[l_1, l_2]$ 的圈上的顶点. 因此，如果用 Σ_A, Σ_{A_1} 和 Σ_{A_2} 分别表示 G_A, G_{A_1} 和 G_{A_2} 的圈元，那么

$$\Sigma_A = \Sigma_{A_1} \cdot \Sigma_{A_2},$$

这里乘积是指在 § 3 中定义的圈元的乘积，即

$$\left(\sum_i N_i[i]\right) \cdot \left(\sum_i N'_i[i]\right) = \sum_{i,j} N_i N'_j (i, j)[[i, j]].$$

于是我们有

定理 4 设 A 是 $n \times n$ 非异矩阵，并设它的初等因子组是

$$p_i(x)^{e_{ij}},\ j = 1, 2, \cdots, r_i,\ \ i = 1, 2, \cdots, s.$$

再令 M_{ij} 是以 $\tilde{p}_i(x)^{e_{ij}}$ 为联接多项式的线性移位寄存器的状态转移矩阵. 那么

$$\Sigma_A = \prod_{i=1}^{s} \prod_{j=1}^{r_i} \Sigma_{M_{ij}},$$

其中 $\Sigma_{M_{ij}}$ 由 § 3 定理 4′ 给出.

再研究幂零矩阵的图. 我们回忆，$n \times n$ 矩阵 A 叫幂零矩

阵，如果有正整数 L 存在使 $A^L=0$. 先举一个例子

例 1 考察 $\mathbf{F}_2$ 上的 4×4 幂零矩阵

$$A=\begin{pmatrix}0&0&0&0\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}.$$

不难作出它的状态图 G_A:

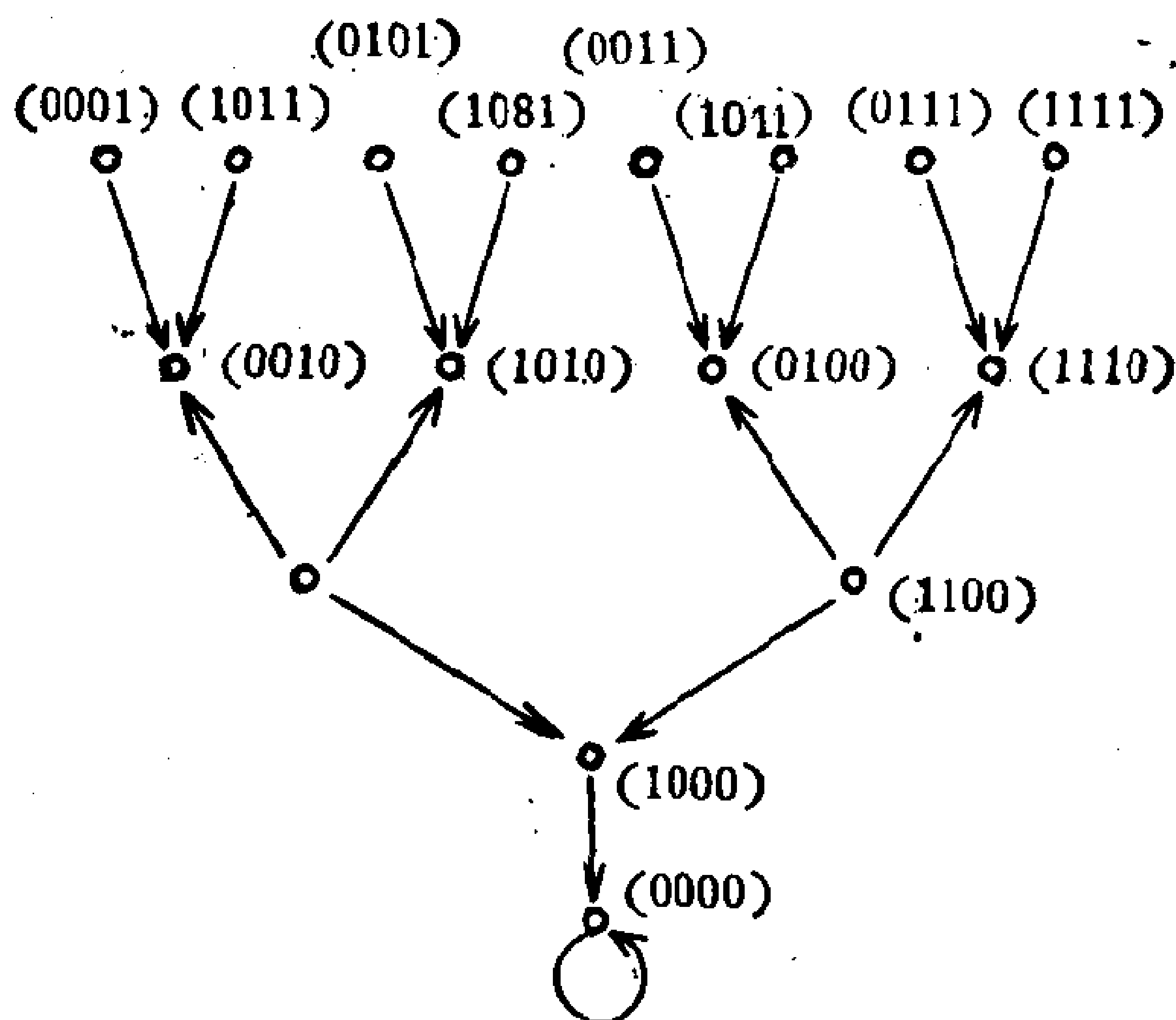


图 5

在 G_A 中有一个长为 1 的圈，它由一条既以 $(0, 0, 0, 0)$ 为起点又以 $(0, 0, 0, 0)$ 为终点的弧组成. 把这个圈取消，我们把剩下的图记作 G'_A. 那么 G'_A 不再有圈. 再注意，对 G'_A 中任一 $\neq(0, 0, 0, 0)$ 的顶点 (a_1, a_2, a_3, a_4)，都有唯一的一串顶点，这串顶点中的头一个是 (a_1, a_2, a_3, a_4)，而最末一个是 $(0, 0, 0, 0)$，使得对于这串顶点中任意两个相邻顶点，G'_A 中都有一条弧以前面的一个顶点为起点，而以后面的一个顶点为终点. 例如，对于 $(1, 1, 1, 1)$，有下面这唯一的一串顶点

$$(1, 1, 1, 1),\ (1, 1, 1, 0),\ (1, 1, 0, 0),$$
$$(1, 0, 0, 0),\ (0, 0, 0, 0)$$

具有上述性质．换句话说，对 G'_A 中任一 $\neq(0, 0, 0, 0)$ 的顶点 (a_1, a_2, a_3, a_4)，都有唯一的一串弧，这串弧里每一条弧（除第一条以外）的起点都是前面一条弧的终点，每一条弧（除最末一条以外）的终点都是后面一条弧的起点，而第一条弧的起点是 (a_1, a_2, a_3, a_4)，最末一条弧的终点是 $(0, 0, 0, 0)$．这样一串弧叫做从 (a_1, a_2, a_3, a_4) 到 $(0, 0, 0, 0)$ 的一条路，而这串弧中弧的个数就叫这条路的长．

一般，我们有

定义 3 设 $G(V, A)$ 是个有向图，x 和 y 是它的两个顶点．如果有一串顶点

$$x=x_1,\ x_2,\ \cdots,\ x_n,\ x_{n+1}=y$$

使得 $(x_i, x_{i+1})\in A$ 对 $i=1, 2, \cdots, n$ 都成立，我们就说下面这串弧

$$(x, x_2),\ (x_2, x_3),\ \cdots,\ (x_n, y)$$

是一条从 x 到 y 的路，而其中弧的个数 n 就叫做这条路的长，

定义 4 设 G 是个有向图．如果 G 有一个顶点，叫做它的根，使得从任意一个不是根的顶点都有唯一一条到根的路，那么 G 就叫做一棵树．如果从 G 的一个不是根的顶点到它的根的路的长等于 l，那么这个顶点就叫一个 l 层顶点，而根叫它的 0 层顶点．一棵树的顶点的层数的极大值就叫这棵树的高度．

例如，例 1 中的 G'_A 就是一棵以 $(0, 0, 0, 0)$ 为根而高度等于 4 的树．

引理 2 设 A 是个 $n\times n$ 幂零矩阵，而 $\mathbf{s}\in V_n(\mathbf{F}_q)$．如果 $\mathbf{s}A=\mathbf{s}$，那么一定有 $\mathbf{s}=0$．

证．设 $A^L=0$，那么 $\mathbf{s}A^L=\mathbf{0}$，如果 $\mathbf{s}A=\mathbf{s}$，那么 $\mathbf{s}A^2=\mathbf{s}A$，$\mathbf{s}A^3=\mathbf{s}A^2$，$\cdots$，$\mathbf{s}A^L=\mathbf{s}A^{L-1}$．因此

$$\mathbf{s}=\mathbf{s}A=\mathbf{s}A^2=\mathbf{s}A^3=\cdots=\mathbf{s}A^{L-1}=\mathbf{s}A^L=\mathbf{0}.$$

定理 5 设 A 是 $\mathbf{F}_q$ 上的 $n\times n$ 幂零矩阵，L 是最小正整数使 $A^{L-1}\neq 0$ 而 $A^L=0$. 那么 A 的图 G_A 由一棵以 $\mathbf{0}$ 为根而高度等于 L 的树 G'_A 和一条以 $\mathbf{0}$ 既为起点又为终点的弧组成. 更进一步，设 A 的初等因子组是

$$\underbrace{x^L, x^L, \cdots, x^L}_{m_L \text{个}}, \underbrace{x^{L-1}, x^{L-1}, \cdots, x^{L-1}}_{m_{L-1} \text{个}}, \cdots, \underbrace{x, x, \cdots, x}_{m_1 \text{个}},$$

而 $L\cdot m_L+(L-1)m_{L-1}+\cdots+1\cdot m_1=n,\ m_i\geqslant 0,\ m_L>0.$

如果用 N_i 表示 G'_A 中 i 层顶点的个数 $(i=0, 1, 2, \cdots, L)$，那么 $N_0=1$ 而

$$N_i=q^{m_1+2m_2+\cdots+(i-1)m_{i-1}+i(m_i+m_{i+1}+\cdots+m_L)}$$
$$-(N_0+N_1+\cdots+N_{i-1}),\ i=1, 2, \cdots, L. \qquad (6)$$

证. 因 $\mathbf{0}A=\mathbf{0}$, 所以 G_A 有一条弧既以 $\mathbf{0}$ 为起点又以 $\mathbf{0}$ 为终点，把这条弧从 G_A 中取消，剩下的有向图记作 G'_A.

我们先来证明 G'_A 是一棵以 $\mathbf{0}$ 为根的树. 这只要证明，对任一非零状态 $\mathbf{s}$, G'_A 都有唯一的一条从 $\mathbf{s}$ 到 $\mathbf{0}$ 的路就行了. 因 $A^L=0$, 故 $\mathbf{s}A^L=\mathbf{0}$. 假定 l 是最小正整数使 $\mathbf{s}A^{l-1}\neq 0$ 而 $\mathbf{s}A^l=\mathbf{0}$. 根据引理 2, $\mathbf{s}$, $\mathbf{s}A$, $\mathbf{s}A^2$, $\cdots$, $\mathbf{s}A^{l-1}$, $\mathbf{s}A^l=\mathbf{0}$ 这 $l+1$ 个状态两两不同，那么以 $\mathbf{s}$ 为起点而以 $\mathbf{s}A$ 为终点的弧，以 $\mathbf{s}A$ 为起点而以 $\mathbf{s}A^2$ 为终点的弧，$\cdots$，和以 $\mathbf{s}A^{l-1}$ 为起点而以 $\mathbf{0}$ 为终点的弧就组成唯一的一条从 $\mathbf{s}$ 到 $\mathbf{0}$ 的路，它的长等于 l.

再证 G'_A 的高度等于 L. 从上一段的证明可知，对 G'_A 中任一 $\neq\mathbf{0}$ 的顶点 $\mathbf{s}$, 从 $\mathbf{s}$ 到 $\mathbf{0}$ 的路的长都 $\leqslant L$. 如果 G'_A 的高度 $L'<L$, 那么根据上一段的证明可知 $\mathbf{s}A^{L'}=\mathbf{0}$ 对任一状态 $\mathbf{s}$. 取 $\mathbf{s}$ 依次为 $(1, 0, 0, \cdots, 0)$, $(0, 1, 0, \cdots, 0)$, $\cdots$, $(0, 0, \cdots, 0, 1)$, 就得到 $A^{L'}=0$, 这与 L 是最小正整数使 $A^L=0$ 相矛盾.

现在来证本定理的最后一个断言. 不妨设 A 是有理标准形来证明它. 令 $i\times i$ 矩阵

$$M(x^i)=\begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & 0 & \\ & & & 1 & 0 \end{pmatrix}$$

并将它简记作 M_i. 那么

$$A=\begin{pmatrix} \underbrace{\begin{matrix} M_L & & \\ & \ddots & \\ & & M_L \end{matrix}}_{m_L\text{个}} & & & & \\ & \underbrace{\begin{matrix} M_{L-1} & & \\ & \ddots & \\ & & M_{L-1} \end{matrix}}_{m_{L-1}\text{个}} & & \\ & & \ddots & \\ & & & \underbrace{\begin{matrix} M_1 & & \\ & \ddots & \\ & & M_1 \end{matrix}}_{m_1\text{个}} \end{pmatrix}$$

根据定义, $N_0=1$. 对于 $i>0$, 令

$$V^i=\{\mathbf{s}\in V_n(\mathbf{F}_q)\,|\,\mathbf{s}A^i=0\},$$

那么

$$|V^i|=N_0+N_1+\cdots+N_i. \tag{7}$$

将 $V_n(\mathbf{F}_q)$ 中的向量 $\mathbf{s}$ 按 A 的分块方式加以分块

$$\mathbf{s}=(\mathbf{s}_{L1},\ \mathbf{s}_{L2},\ \cdots,\ \mathbf{s}_{Lm_L},\ \mathbf{s}_{L-1,1},\ \mathbf{s}_{L-1,2},\ \cdots,\\ \mathbf{s}_{L-1,m_{L-1}},\ \cdots,\ \mathbf{s}_{11},\ \mathbf{s}_{12},\ \cdots,\ \mathbf{s}_{1m_1}),$$

其中 $\mathbf{s}_{jk}(k=1,\ 2,\ \cdots,\ m_j)$, 都是 j 维行向量, $j=1,\ 2,\ \cdots,L$. 那么易证 $\mathbf{s}\in V^i(1\leqslant i\leqslant L)$, 当且仅当 $\mathbf{s}_{jk}(k=1,\ 2,\ \cdots,\ m_j,$

$j=1, 2, \cdots, i$)是任意 j 维行向量，而 $\mathbf{s}_{jk}$ ($k=1, 2, \cdots, m_j$, $j=i+1, \cdots, L$)的前 i 个分量任意而后 $j-i$ 个分量等于0. 因此

$$|V^i| = q^{m_1+2m_2+\cdots+(i-1)m_{i-1}+i(m_i+m_{i+1}+\cdots+m_L)} \tag{8}$$

由(7)，(8)两式立刻推出(6)式.

定义5 在一棵树中，如果从顶点 x 到顶点 y 有一条长为 l 的路，我们就说 x 是 y 的 l 级先导，而 y 是 x 的 l 级后继.

系理1 在定理5的假设下，G'_A 的任一非零状态的 i 级先导的个数或者等于0或者等于 $N_0+N_1+\cdots+N_i$. 更进一步，G'_A 中只有 $(q^n/(N_0+N_1+\cdots+N_i))-1$ 个非零状态的 i 级先导的个数不等于0而等于 $N_0+N_1+\cdots+N_i$.

证. 设 $\mathbf{s}$ 是 G_A 的任一状态. 令

$$V^i_{\mathbf{s}} = \{\mathbf{v}\in V_n(\mathbf{F}_q)\,|\,\mathbf{v}A^i=\mathbf{s}\}.$$

当 $\mathbf{s}\neq\mathbf{0}$ 时，$V^i_{\mathbf{s}}$ 就是 G'_A 中 $\mathbf{s}$ 的 i 级先导的全体组成的集合，而当 $\mathbf{s}=\mathbf{0}$ 时，$V^i_0=V^i$.

显然 V^i 是 $V_n(\mathbf{F}_q)$ 的子空间. 我们再证明，当 $\mathbf{s}\neq\mathbf{0}$ 时，如果 $V^i_{\mathbf{s}}$ 非空，$V^i_{\mathbf{s}}$ 就是 $V_n(\mathbf{F}_q)$ 对于 V^i 的一个陪集. 任选 $\mathbf{v}_0\in V^i_{\mathbf{s}}$，那么 $\mathbf{v}_0A^i=\mathbf{s}$，再设 $\mathbf{v}$ 是 $V^i_{\mathbf{s}}$ 中任一向量，也有 $\mathbf{v}A^i=\mathbf{s}$. 于是 $(\mathbf{v}-\mathbf{v}_0)A^i=\mathbf{0}$，因此 $\mathbf{v}-\mathbf{v}_0\in V^i$，即 $\mathbf{v}\in\mathbf{v}_0+V^i$. 这证明 $V^i_{\mathbf{s}}\subset\mathbf{v}_0+V^i$. 反过来，对任一 $\mathbf{v}_0+\mathbf{u}\in\mathbf{v}_0+V^i$，这里 $\mathbf{u}\in V^i$，我们有 $(\mathbf{v}_0+\mathbf{u})A^i=\mathbf{s}$. 因此 $\mathbf{v}_0+V^i\subset V^i_{\mathbf{s}}$. 所以 $V^i_{\mathbf{s}}=\mathbf{v}_0+V^i$. 由此立刻推出

$$|V^i_{\mathbf{s}}| = |V^i| = N_0+N_1+\cdots+N_i.$$

更进一步，设 $\mathbf{v}_1+V^i$ 是 $V_n(\mathbf{F}_q)$ 对于 V^i 的任一陪集，而 $\mathbf{v}_1\notin V^i$. 令 $\mathbf{v}_1A^i=\mathbf{s}_1$，那么 $\mathbf{s}_1\neq 0$ 而 $\mathbf{v}_1\in V^i_{\mathbf{s}_1}$. 再根据上一段的讨论可知，$V^i_{\mathbf{s}_1}=\mathbf{v}_1+V^i$，因此 G'_A 中 i 级先导的个数 $\neq 0$ 的非零状态的个数等于

$$(V_n(\mathbf{F}_q):V^i)-1,$$

而 $$V_n(\mathbf{F}_q):V_i=q^n/(N_0+N_1+\cdots+N_i)$$

系理 2 $(N_0+N_1+\cdots+N_i)\mid N_{i+1},\ i=1, 2, \cdots, L-1.$

证. 根据定理 5.

$$N_{i+1}=q^{m_1+2m_2+\cdots+im_i+(i+1)(m_{i+1}+m_{i+2}+\cdots+m_L)}-(N_0+N_1+\cdots+N_i),$$

$$N_0+N_1+\cdots+N_i=q^{m_1+2m_2+\cdots+(i-1)m_{i-1}+i(m_i+m_{i+1}+\cdots+m_L)}.$$

因

$$m_1+2m_2+\cdots+(i-1)m_{i-1}+i(m_i+m_{i+1}+\cdots+m_L)$$
$$\leqslant m_1+2m_2+\cdots+im_i+(i+1)(m_{i+1}+m_{i+2}+\cdots+m_L),$$

所以 $$(N_0+N_1+\cdots+N_i)\mid N_{i+1}.$$

在定理 5 的假设下，设 $\mathbf{x}$ 是 G_A 的一个非零顶点，并假定 $\mathbf{x}$ 有 l 级先导. 用 $G_A(\mathbf{x}, l)$ 表 G_A 的子图，它的顶点集由 $\mathbf{x}$ 和 $\mathbf{x}$ 的所有 1 级，2 级，…，l 级先导组成，而它的弧集由所有以 $\mathbf{x}$ 的 1 级，2 级，…，l 级先导为起点的弧组成. 那么我们有

系理 3 在定理 5 的假设下，设 $\mathbf{x}$ 是 G_A 的一个非零顶点，并假定 $\mathbf{x}$ 有 l 级先导，那么 $G_A(\mathbf{x}, l)$ 是一棵高度等于 l 的树，而它的 i 层顶点 $(0\leqslant i\leqslant l)$ 的个数等于 $N_0+N_1+\cdots+N_i$. 更进一步，如果 y 也是 G_A 的一个非零顶点，而 y 也有 l 级先导，那么 $G_A(\mathbf{x}, l)$ 和 $G_A(\mathbf{y}, l)$ 同构.

证. 显然 $G_A(\mathbf{x}, l)$ 是一棵树 0，而树的高度等于 l. 根据系理 1，$\mathbf{x}$ 的 i 级先导的个数等于 $N_0+N_1+\cdots+N_i$. 因 $\mathbf{x}$ 的 i 级先导即是 $G_A(x, l)$ 的 i 层顶点，所以 $G_A(\mathbf{x}, l)$ 的 i 层顶点的个数也等于 $N_1+N_2+\cdots+N_i$

现在来证明本系理的第二个断言. 对 l 用归纳法来证明. 当 $l=1$ 时，$G_A(\mathbf{x}, 1)$ 和 $G_A(\mathbf{y}, 1)$ 都是高度等于 1 的树，而它们 1 层顶点的个数都等于 N_0+N_1，所以它们同构.

现在假定 $l>1$. 根据系理 1，$G_A(\mathbf{x}, l)$ 和 $G_A(\mathbf{y}, l)$ 的 1

层顶点的个数都等于 N_0+N_1. 更进一步，对任意 $i=1, 2, \cdots, l-1$, $G_A(\mathbf{x}, l)$和 $G_A(\mathbf{y}, l)$的 $i+1$ 层顶点的个数都等于 $N_0+N_1+\cdots+N_{i+1}$, 而它们的 1 层顶点中有 i 级先导的个数或者等于 0 或者等于 $N_0+N_1+\cdots+N_i$; 因此它们的 1 层顶点中有 i 级先导的个数都等于 $(N_0+N_1+\cdots+N_{i+1})/(N_0+N_1+\cdots+N_i)$. 由此推出，对 $i=0, 1, 2, \cdots, l-1$, $G_A(\mathbf{x}, l)$ 和 $G_A(\mathbf{y}, l)$ 的 1 层顶点中有 i 级先导而没有 $i+1$ 先导的个数也相等. 不妨设

$$\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_{N_0+N_1} \text{ 和 } \mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_{N_0+N_1}$$

分别是 $G_A(\mathbf{x}, l)$ 和 $G_A(\mathbf{y}, l)$ 的 1 层顶点的集合，其中

$$\mathbf{x}_{n_i+1}, \cdots, \mathbf{x}_{n_{i+1}} \text{ 和 } \mathbf{y}_{n_i+1}, \cdots, \mathbf{y}_{n_{i+1}},$$

$$i=0, 1, 2, \cdots, l-1,$$

分别是其中有 i 级先导而没有 $i+1$ 级先导的 1 层顶点，那么

$$n_0=0\leqslant n_1\leqslant n_2\leqslant\cdots\leqslant n_l=N_0+N_1.$$

根据归纳法假设 $G_A(\mathbf{x}_{n_i+j,i})$ 和 $G_A(\mathbf{y}_{n_i+j,i})$ $(j=1, 2, \cdots, n_{i+1}-n_i;\ i=0, 1, 2, \cdots, l-1)$两两同构. 由这些同构即可造出 $G_A(\mathbf{x}, l)$ 和 $G_A(\mathbf{y}, l)$ 之间的一个同构.

利用定理 5 和它的系理，我们可以得到一个作幂零矩阵的图的算法：设 A 是 $n\times n$ 幂零矩阵，按定理 5 算出 G_A 的各层顶点的个数 $N_0, N_1, N_2, \cdots$. 先画出 $\mathbf{0}$ 以及以 $\mathbf{0}$ 既为起点又为终点的弧. 再画出 G_A 的 N_1 个 1 层顶点并画出以 1 层顶点为起点的弧，这一共 N_1 条弧. 假定 G_A 的层数 $<l$ 的顶点以及以它们为起点的弧都已经画出. 现在画出 G_A 的 N_l 个 l 层顶点. 先将它们分成一些 1 级组，每组含 $N_0+N_1+\cdots+N_{l-1}$ 个顶点. 选出 $N_l/(N_0+N_1+\cdots+N_{l-1})$ 个有 $l-2$ 级先导的 1 层顶点，令每个 1 级组相应于选出的一个 1 层顶点，并假定这个 1 级组中的顶点是它相应的 1 层顶点的 $l-1$ 级先导. 再将每个 1 级组分成一些 2 级组，每组含 $N_0+N_1+\cdots$

$+N_{l-2}$ 个顶点. 从刚才选出来的相应于一个 1 级组的 1 层顶点的先导(注意, 它们是 2 层顶点)中选出 $(N_0+N_1+\cdots+N_{l-1})/(N_0+N_1+\cdots+N_{l-2})$ 个有 $l-3$ 级先导的来, 令每个 2 级组相应于选出的一个 2 层顶点, 并假定这个 2 级组中的顶点是它相应的 2 层顶点的 $l-2$ 级先导. 如此继续下去, 直到 l 层顶点分成一些 $l-1$ 级组, 每组含 N_0+N_1 个顶点, 每个 $l-1$ 级组中的顶点都被认为是某个 $l-1$ 层顶点的后继. 这样就作出了以 l 层顶点为起点的弧. 于是归纳地就可以作出 A 的图 G_A (确切地说, 是作出了与 G_A 同构的一个图).

例 2 作出 $\mathbf{F}_2$ 上 5×5 幂零矩阵

$$A=\begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & & 0 & \\ & & & 1 & 0 \end{pmatrix}$$

的图

这时 $m_1=0,\ m_2=1,\ m_3=1.$

于是 $N_0=1,$

$$N_1=2^{1\cdot(0+1+1)}-N_0=2^2-1=3,$$

$$N_2=2^{2\cdot(1+1)}-(N_0+N_1)=2^4-(1+3)=12,$$

$$N_3=2^{2\cdot1+3\cdot1}-(N_0+N_1+N_2)$$

$$=2^5-(1+3+12)=16.$$

先画出 1 个 0 层顶点和以它为起点及终点的弧.

再画出 3 个 1 层顶点, 和这 3 个 1 层顶点为起点而以 0 层顶点为终点的 3 条弧.

再画出 12 个 2 层顶点. 我们把这 12 个 2 层顶点平均分成 $N_2/(N_0+N_1)=3$ 个 1 级组, 每组 4 个 2 层顶点是一个 1 层顶点的 1 级先导, 这就是说 G_A 的 3 个 1 层顶点中的每一个

都有 4 个 2 层顶点作为它的 1 级先导. 这样就可以画出以这 12 个 2 层顶点为起点的弧.

再画出 16 个 3 层顶点. 把这 16 个 3 层顶点分成 $N_3/(N_0+N_1+N_2)=1$ 个 1 级组，它们是一个 1 层顶点的 2 级先导. 因 3 个 1 层顶点都有 1 级先导，故可以从 3 个 1 层顶点中任选出一个来，并设它有 16 个 2 级先导. 再将 1 级组中的 16 个顶点分成 $(N_0+N_1+N_2)/(N_0+N_1)$ 个 2 级组，每组含 4 个顶点，每个 2 级组中的顶点是上面选出的那个 1 层顶点的 1 级先导(它们本身是 2 层顶点)的 1 级先导. 这样就可以画出以这 16 个 3 级顶点为起点的弧.

结果我们得到 A 的图 G_A:

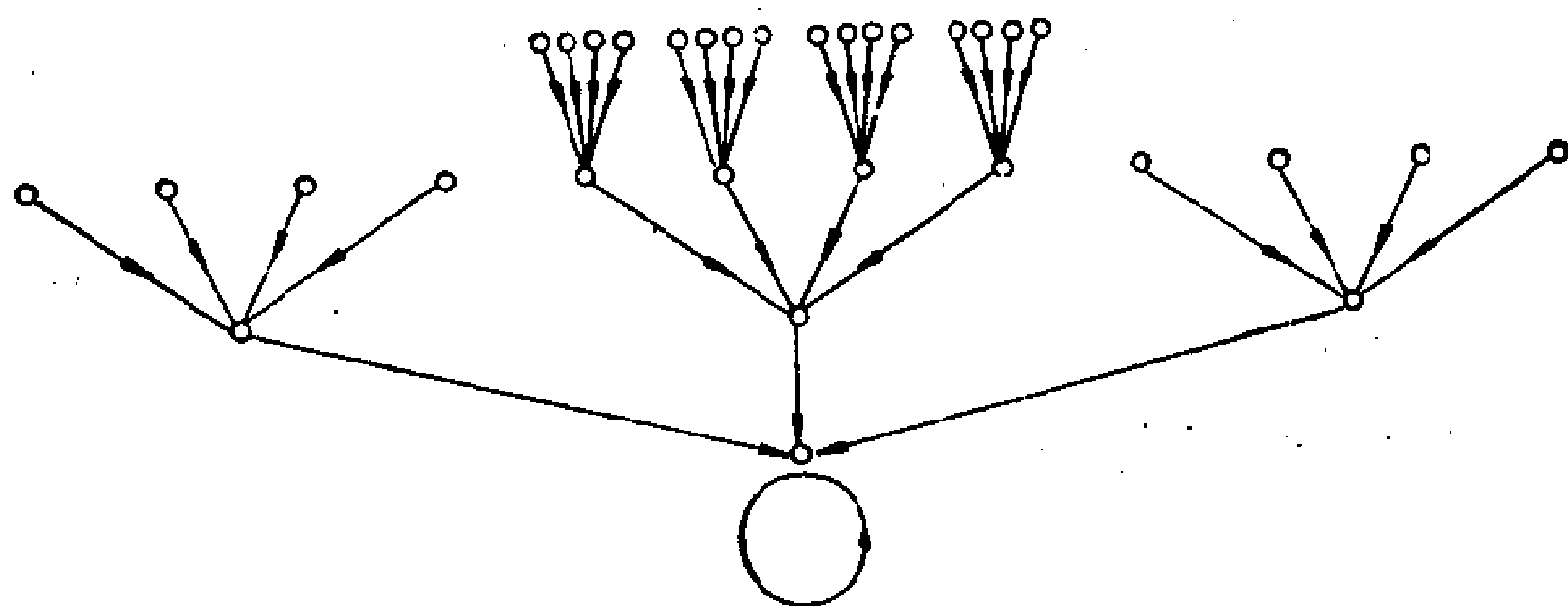


图 6

前面我们已经分别讨论了作 $\mathbf{F}_q$ 上非异矩阵和幂零矩阵的图的方法. 现在设 A 是 $\mathbf{F}_q$ 上的任意 $n\times n$ 矩阵. 我们来讨论作 A 的图的方法. 根据定理 1，可以设 A 是有理标准形. 令

$$A=\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

其中 A_1 是个 $n_1\times n_1$ 幂零矩阵，A_2 是个 $n_2\times n_2$ 非异矩阵，而 $n_1+n_2=n$. 我们知道怎样作 A_1 的图 G_{A_1}，而 G_{A_1} 由一棵以

$$\mathbf{O}_1=\underbrace{(0,\ 0,\ \cdots,\ 0)}_{n_1\text{个}0}$$

为根的树和一条以 $\mathbf{O}_1$ 既为起点又为终点的弧组成. 我们也

知道怎样作 A_2 的图 G_{A_2}，而 G_{A_2} 由一些两两没有公共顶点的圈组成. G_A 的顶点集是 $V_n(\mathbf{F}_q)$. 问题是怎样作出 G_A 的弧. 令

$$V^{(2)}=\{(\mathbf{O}_1,\ \mathbf{s}_2)\,|\,\mathbf{s}_2\in V_{n_2}(\mathbf{F}_q)\},$$
$$A^{(2)}=\{((\mathbf{O}_1,\ \mathbf{s}_2),\ (\mathbf{O}_1,\ \mathbf{s}_2)A)\,|\,\mathbf{s}_2\in V_{n_2}(\mathbf{F}_q)\}$$
$$G^{(2)}=G(V^{(2)},\ A^{(2)}).$$

那么 $G^{(2)}$ 是个有向图，而映射

$$\mathbf{s}_2\to(\mathbf{O}_1,\ \mathbf{s}_2)$$

是从 G_{A_2} 到 $G^{(2)}$ 之上的一个同构. 对 $\mathbf{s}_1\in V_{n_1}(\mathbf{F}_q)$，用 $d(\mathbf{s}_1)$ 表 $\mathbf{s}_1$ 作为 G'_{A_1} 的顶点的层数. 再设 $\mathbf{s}_2$ 是 $V_n(\mathbf{F}_q)$ 中任意选定的一个向量. 令

$$V(\mathbf{s}_2)=\{(\mathbf{s}_1,\ \mathbf{s}_2A_2^{-d(\mathbf{s}_1)})\,|\,\mathbf{s}_1\in V_n(\mathbf{F}_q)\},$$
$$A(\mathbf{s}_2)=\{((\mathbf{s}_1,\ \mathbf{s}_2A_2^{-d(\mathbf{s}_1)}),\ (\mathbf{s}_1,\ \mathbf{s}_2A^{-d(\mathbf{s}_1)})A)$$
$$|\,\mathbf{s}_1\in V_{n_1}(\mathbf{F}_q)\ \text{而}\ \mathbf{s}_1\neq 0\},$$
$$G(\mathbf{s}_2)=G(V(\mathbf{s}_2),\ A(\mathbf{s}_2)),$$

那么 $G(\mathbf{s}_2)$ 是个有向图，而映射

$$\mathbf{s}_1\to(\mathbf{s}_1,\ \mathbf{s}_2A_2^{-d(\mathbf{s}_1)})$$

是从 G'_{A_1} 到 $G(\mathbf{s}_2)$ 之上的一个同构. 显然 $V(\mathbf{s}_2)(\mathbf{s}_2\in V_{n_2}(\mathbf{F}_q))$ 两两没有公共顶点，而

$$V_n(\mathbf{F}_q)=\bigcup_{\mathbf{s}_2\in V_{n_2}(\mathbf{F}_q)}V(\mathbf{s}_2).$$

显然 $A^{(2)}$, $A(\mathbf{s}_2)(\mathbf{s}_2\in V_{n_2}(\mathbf{F}_q))$ 也两两没有公共弧，而

$$A^{(2)}\cup(\bigcup_{\mathbf{s}_2\in V_{n_2}(\mathbf{F}_q)}A(\mathbf{s}_2))$$

正好是 G_A 的弧的集合. 所以 G_A 正好是它的子图 $G^{(2)}$, $G(\mathbf{s}_2)$ $(\mathbf{s}_2\in V_{n_2}(\mathbf{F}_q))$ 的并. 因此为了造 G_A，只要先造出 G_{A_2}，然后以 G_{A_2} 的每个顶点为根造一棵与 G'_{A_1} 同构的树，这样就得到 G_A（确切地说，是得到与 G_A 同构的一个图).

下面我们来讨论一般的自律线性时序线路，即有输出的

自律线性时序线路. 下面是有n个寄存器和m个输出端的自律时序线路的框图

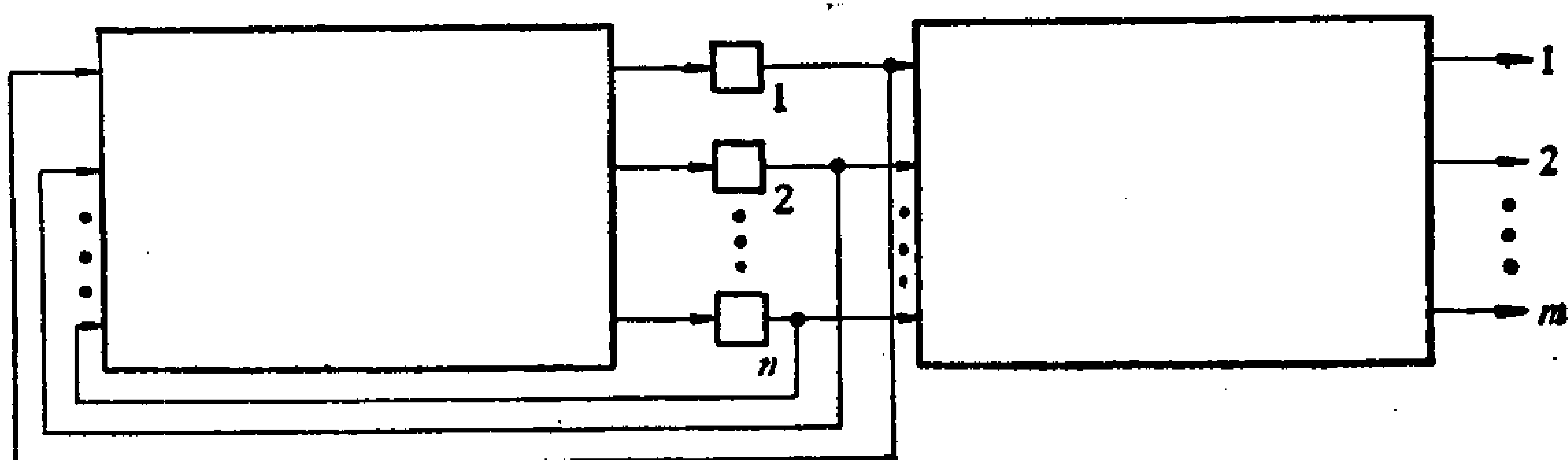


图 7

这个图与图4不同的地方在于多了右边的一个长方框，它代表一个有n个输入端、m个输出端的开关线路，叫做输出开关线路. 设在时刻t, n个寄存器的内容从上到下依序是$s_1(t)$, $s_2(t)$, $\cdots$, $s_n(t)$, 即这个自律时序线路的状态是

$$\mathbf{s}(t)=(s_1(t),\ s_2(t),\ \cdots,\ s_n(t)),$$

而$\mathbf{s}(t)\in V_n(\mathbf{F}_q)$. 再设在时刻$t$, 输出开关线路的$m$个输出端的输出从上到下依序是$y_1(t)$, $y_2(t)$, $\cdots$, $y_m(t)$, 它们也是$\mathbf{F}_q$中的元素, 那么

$$y_j(t+1)=g_j(s_1(t),\ s_2(t),\ \cdots,\ s_n(t)),\quad j=1,\ 2,\ \cdots,\ m, \tag{9}$$

而g_1, g_2, $\cdots$, g_m都是定义在$V_n(\mathbf{F}_q)$上而在$\mathbf{F}_q$中取值的n元(开关)函数, 它们由输出开关线路完全确定. 我们说这个自律时序线路在时刻t的输出是

$$\mathbf{y}(t)=(y_1(t),\ y_2(t),\ \cdots,\ y_m(t)),$$

而$\mathbf{y}(t)$可以看作$V_m(\mathbf{F}_q)$中的向量. 另外, 和本节一开始时讨论的无输出的自律时序线路一样, 在时刻$t+1$, 这个自律时序线路的状态$\mathbf{s}(t+1)$是

$$\mathbf{s}(t+1)=(f_1(\mathbf{s}(t)),\ f_2(\mathbf{s}(t)),\ \cdots,\ f_n(\mathbf{s}(t))), \tag{10}$$

其中f_1, f_2, $\cdots$, f_n都是定义在$V_n(\mathbf{F}_q)$上而在$\mathbf{F}_q$中取值

的 n 元(开关)函数，它们由自律时序线路的反馈开关线路完全确定.

当上述自律时序线路的 $n+m$ 个开关函数 $f_1, f_2, \cdots, f_n, g_1, g_2, \cdots, g_m$ 都是线性齐次函数时，即

$$f_j(x_1, x_2, \cdots, x_n)=\sum_{i=1}^{n} a_{ij}x_i,\ a_{ij}\in \mathbf{F}_q,\ j=1, 2, \cdots, n,$$

$$g_k(x_1, x_2, \cdots, x_n)=\sum_{i=1}^{n} c_{ij}x_i,\ c_{ij}\in \mathbf{F}_q,\ k=1, 2, \cdots, m,$$

我们就说上述自律时序线路是自律线性时序线路. 令

$$A=(a_{ij})_{1\le i,j\le n},\quad C=(c_{ik})_{1\le i\le n, 1\le k\le m},$$

那么(10), (9)两式可写作

$$\mathbf{s}(t+1)=\mathbf{s}(t)A \tag{11}$$

$$\mathbf{y}(t+1)=\mathbf{s}(t)C \tag{12}$$

A 仍叫这个自律线性时序线路的状态转移矩阵，而 C 叫它的输出开关线路的矩阵.

给定上述自律线性时序线路的初始状态 $\mathbf{s}(0)$ 之后，当 t 依序取 1, 2, 3, ⋯ 诸值时，它的输出就是 $\mathbf{F}_q$ 上的一个 m 维行向量序列

$$\mathbf{y}(1), \mathbf{y}(2), \mathbf{y}(3), \cdots,$$

或它的 m 个输出端的输出就是 m 个 q 元序列

$$y_k(1), y_k(2), y_k(3), \cdots, k=1, 2, \cdots, m \tag{13}$$

我们把 A 的极小多项式记作 $m(x)$，设 $\partial^0 m(x)=n_0$, 可以写

$$m(x)=x^{n_0}+c_1x^{n_0-1}+c_2x^{n_0-2}+\cdots+c_{n_0}.$$

由 $m(A)=0$ 推出

$$\mathbf{s}(t)m(A)=0,\ t=0, 1, 2, \cdots$$

即 $\mathbf{s}(t+n_0)+c_1\mathbf{s}(t+n_0-1)+c_2\mathbf{s}(t+n_0-2)+\cdots+c_{n_0}\mathbf{s}(t)=0,$

$$t=0, 1, 2, \cdots,$$

也即

$$s_j(t+n_0)+c_1s_j(t+n_0-1)+c_2s_j(t+n_0-2)+\cdots+c_{n_0}s_j(t)=0,$$
$$t=0,\ 1,\ 2,\ \cdots,\quad j=1,\ 2,\ \cdots,\ n.$$

换句话说,

$$s_j(0),\ s_j(1),\ s_j(2),\ \cdots,\ j=1,\ 2,\ \cdots,\ n \tag{14}$$

这m个 q 元序列都适合线性递归关系式

$$a_k+c_1a_{k-1}+c_2a_{k-2}+\cdots+c_{n_0}a_{k-n_0}=0,\ k\geqslant n_0. \tag{15}$$

由(12)式可知, m 个输出序列(13)都是(14)中 n 个序列的线性组合, 因此它们也适合线性递归关系式(15); 换句话说, 它们都可以由以

$$f(x)=1+c_1x+c_2x^2+\cdots+c_{n_0}x^{n_0}$$

为联接多项式的 q 元 n_0 级线性移位寄存器从适当选取的初态出发产生.

反过来,设

$$a_0,\ a_1,\ a_2,\ \cdots \tag{16}$$

是由以$f(x)$ 为联接多项式的 q 元 n_0 级线性移位寄存器以$(a_0,\ a_1,\ \cdots,\ a_{n_0-1})$ 为初态产生的一个 q 元序列. 我们要证明, 对于状态转移矩阵的极小多项式为 $m(x)$ 的任一无输出的自律线性时序线路, 总可以选择一个只有一个输出端的线性输出开关线路, 使得这个自律线性时序线路从某个初态出发,所产生的输出序列正好是(16).

先考察这个自律线性时序线路的状态转移矩阵 A 是有理标准形的情形. 设 A 的初等因子组是

$$p_i(x)^{e_{ij}},\ j=1,\ 2,\ \cdots,\ r_i,\ i=1,\ 2,\ \cdots,\ s,$$

其中 $p_1(x)=x,\ p_2(x),\ \cdots,\ p_s(x)$是 s 个两两不同的不可约多项式,而

$$e_{11}\geqslant e_{12}\geqslant\cdots\geqslant e_{1r_1}\geqslant 0$$
$$e_{i1}\geqslant e_{i2}\geqslant\cdots\geqslant e_{ir_i}>0,\ i=2,\ 3,\ \cdots,\ s.$$

沿用定理 2 的证明中的记号 n_{ij}, $p_i(x)^{n_{ij}}$ 和 M_{ij}, 并假定 A 就

是定理 2 的证明中的矩阵(5). 那么 A 的极小多项式 $m(x)$ 就等于

$$m(x)=x^{n_{11}}p_2(x)^{n_{21}}\cdots p_s(x)^{n_{s1}}.$$

令

$$k_1=1,$$

$$k_2=\sum_{j=1}^{r_1}n_{1j}+1,$$

$$k_3=\sum_{j=1}^{r_1}n_{1j}+\sum_{j=1}^{r_2}n_{2j}+1,$$

$$\cdots\cdots\cdots\cdots$$

$$k_s=\sum_{i=1}^{s-1}\sum_{j=1}^{r_i}n_{ij}+1.$$

那么以 A 为状态转移矩阵的自律线性时序线路，当给定初态以后，对 $i=2, 3, \cdots, s$, 它的第 k_i 个延迟元件在时刻 1, 2, 3, ⋯ 的输出就是 $G(f_{i1})$ 中的序列，而这里 $f_{i1}(x)=\tilde{p}_i(x)^{e_{i1}}$; 对于所有可能的初态，它的 k_i 个延迟元件的输出序列的全体就是 $G(f_{i1})$. 因 $f_{21}(x)$, $f_{31}(x)$, ⋯, $f_{s1}(x)$ 这 $s-1$ 个多项式两两互素，根据 § 3 定理 2,

$$G(f_{21}\cdot f_{31}\cdot\cdots\cdot f_{s1})=G(f_{21})\dot{+}G(f_{31})\dot{+}\cdots\dot{+}G(f_{s1}).$$

可以适当改变(16)的前 n_{11} 项，使得所得序列

$$\mathbf{a}'=(a_0', a_1', \cdots, a_{n_{11}-1}', a_{n_{11}}, a_{n_{11}+1}, a_{n_{11}+2}, \cdots)$$

属于 $G(f_{21}\cdot f_{31}\cdot\cdots\cdot f_{s1})$. 令

$$\mathbf{a}'=\mathbf{a}_2+\mathbf{a}_3+\cdots+\mathbf{a}_s,$$

而 $\mathbf{a}_i=(a_{i0}, a_{i1}, a_{i2}, \cdots)\in G(f_{i1}),\ i=2, 3, \cdots, s.$

那么在以 A 为状态转移矩阵的自律线性时序线路的第 1 个至第 n_{11} 个寄存器中依序置 a_0-a_0', a_1-a_1', ⋯, $a_{n_{11}-1}-a_{n_{11}-1}'$, 在第 k_i 个至第 k_i+n_{i1-1} 个寄存器中依次置 a_{i0}, a_{i1}, ⋯, $a_{in_{i1}-1}$ ($i=2, 3, \cdots, s$), 并在其余寄存器中都置 0; 从这样选取的初态出发，如果选择输出开关线路是

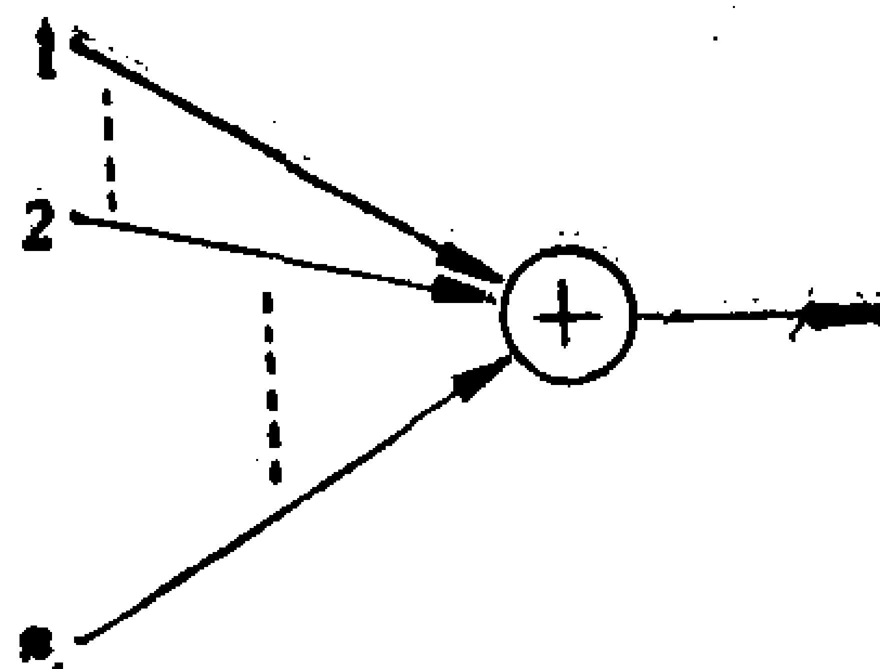


图 8

所得的输出序列正好是(16).

再考察一般情形. 这时可设有可逆矩阵 P 存在使 $B=P^{-1}AP$ 为有理标准形. 根据上面一段的讨论, 可以选择下面这个自律线性时序线路的初态 $\mathbf{s}(0)$, 使它的输出是事先给定的序列(16).

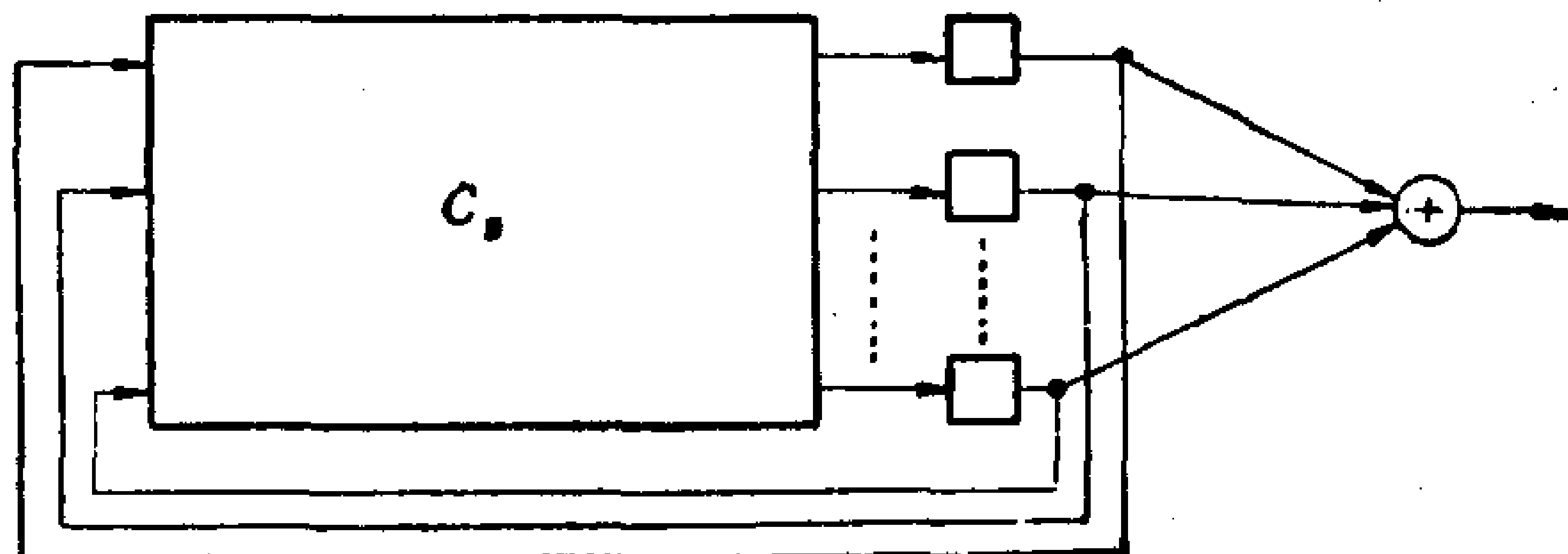


图 9

那么选择下面这个自律线性时序线路的初态 $\mathbf{s}(0)P^{-1}$, 它的输出序列也是事先给定的序列(16).

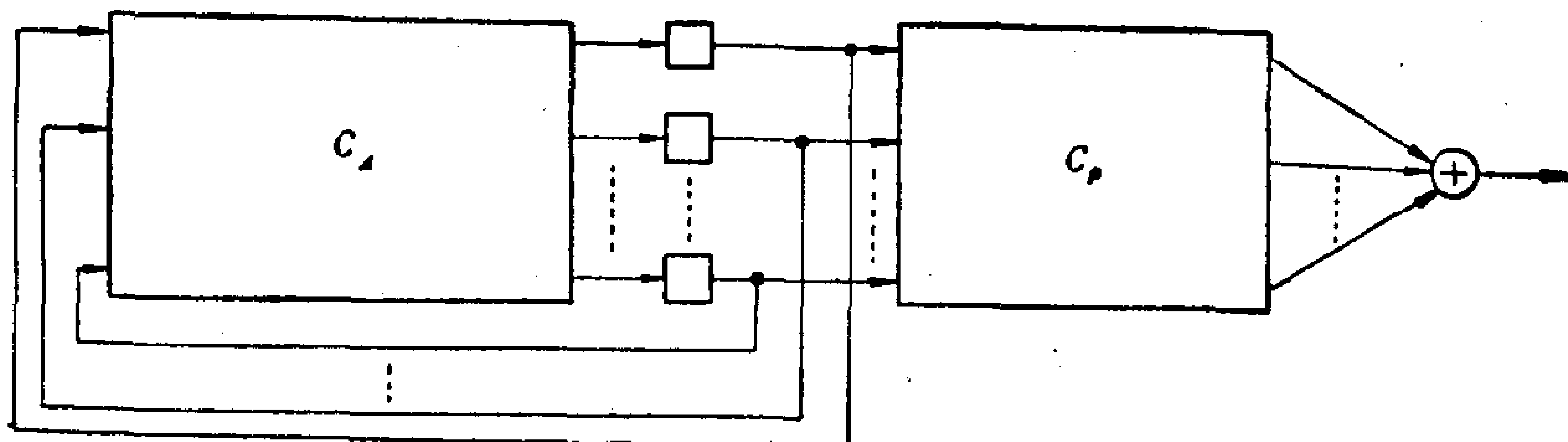


图 10

这样我们就证明下面这个定理.

定理 6 设有一自律线性时序线路, 它的状态转移矩阵

是 A，而 A 的极小多项式是 $m(x)$．令 $\partial^0 m(x)=n_0$，写

$$m(x)=x^{n_0}+c_1x^{n_0-1}+c_2x^{n_0-2}+\cdots+c_{n_0}.$$

再令 $$f(x)=1+c_1x+c_2x^2+\cdots+c_{n_0}x^{n_0}.$$

那么从这个自律线性时序线路的任一初始状态出发，它的任一输出序列都可以由以 $f(x)$ 为联接多项式的 n_0 级线性移位寄存器产生．反过来，任给一由以 $f(x)$ 为联接多项式的 n_0 级线性移位寄存器产生的 q 元序列，总可以选择这个自律线性时序线路的一个只有一个输出端的输出线性开关线路，使得它从某一初始状态出发就产生事先给定的 q 元序列．

最后，我们再指出，由方程(11)，(12) 所描述的自律线性时序线路的 m 个输出序列的初态

$$(y_k(1),\ y_k(2),\ \cdots,\ y_k(n_0)),\ k=1,\ 2,\ \cdots,\ m,$$

可以用自律线性时序线路的初态 $\mathbf{s}(0)$ 表出．我们有

$$\mathbf{y}(1)=\mathbf{s}(0)C,$$

$$\mathbf{y}(2)=\mathbf{s}(1)C=\mathbf{s}(0)AC,$$

$$\mathbf{y}(3)=\mathbf{s}(2)C=\mathbf{s}(0)A^2C,$$

$$\cdots$$

$$\mathbf{y}(n_0)=\mathbf{s}(n_0-1)C=\mathbf{s}(0)A^{n_0-1}C.$$

如果把 C 的第 k 列记作 $\mathbf{c}_k'$，那么

$$(y_k(1),\ y_k(2),\ \cdots,\ y_k(n_0))=(\mathbf{s}(0)\mathbf{c}_k',\ \mathbf{s}(0)A\mathbf{c}_k',\ \cdots,\ \mathbf{s}(0)A^{n_0-1}\mathbf{c}_k')$$

特别，当 $m=n$ 而 $C=I^{(n)}$ 时，

$$(y_k(1),\ y_k(2),\ \cdots,\ y_k(n_0))=(\mathbf{s}(0)\mathbf{e}_k',\ \mathbf{s}(0)A\mathbf{e}_k',\ \cdots,\ \mathbf{s}(0)A^{n_0-1}\mathbf{e}_h'),$$

其中 $$\mathbf{e}_k=(0,\ \cdots,\ 0,\ \underset{\text{第}k\text{分量}}{1},\ 0,\ \cdots,\ 0).$$

下面我们举几个自律线性时序线路的例子，并应用上面介绍的理论对它们进行讨论.

例 3 线性移位寄存器的并联.

设有两个 q 元线性移位寄存器，一个是 n_1 级的，另一个是 n_2 级的. 再设它们的联接多项式分别是

$$f_1(x)=1+c_{11}x+c_{12}x^2+\cdots+c_{1n_1}x^{n_1},$$
$$c_{1i}\in\mathbf{F}_q,\ i=1,\ 2,\ \cdots,\ n_1,$$
$$f_2(x)=1+c_{21}x+c_{22}x^2+\cdots+c_{2n_2}x^{n_2},$$
$$c_{2i}\in\mathbf{F}_q,\ i=1,\ 2,\ \cdots,\ n_2.$$

将这两个线性移位寄存器并联如下:

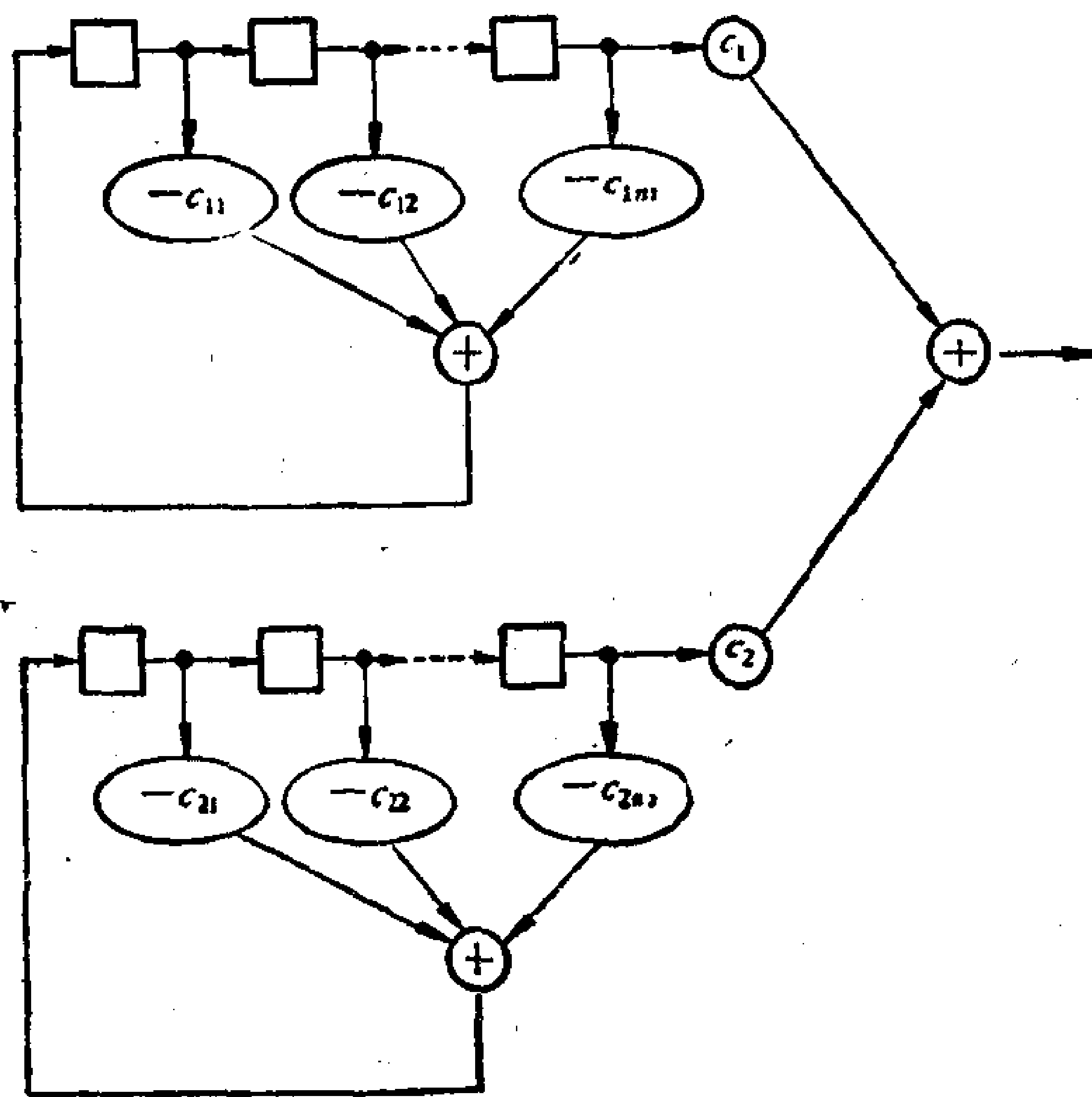


图 11

其中 $c_1,\ c_2\in\mathbf{F}_q$. 令 $n=n_1+n_2$，那么图 11 可以看成是有 n 个寄存器和一个输出的自律线性时序线路. 把上面一排寄存器从右到左依序叫做第 1 个，第 2 个，…，第 n_1 个寄存器；把下

面一排寄存器从右到左依序叫做第 n_1+1 个，第 n_1+2 个，…，第 n 个寄存器．那么这个自律线性时序线路的状态转移矩阵就可以写作

$$A=\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

其中 A_i 是 $n_i\times n_i$ 矩阵

$$A_i=\begin{pmatrix} 0 & & & & -c_{in_i} \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -c_{i2} \\ & & & 1 & -c_{i1} \end{pmatrix},\ i=1,\ 2.$$

令 $\qquad g_i(x)=x^{n_i}+c_{i1}x^{n_i-1}+c_{i2}x^{n_i-2}+\cdots+c_{in_i},\ i=1,\ 2.$

那么 $g_i(x)$ 既是 A_i 的特征多项式又是 A_i 的极小多项式*.

令

$$g(x)=[g_1(x),\ g_2(x)]$$

那么 $g(x)$ 就是 A 的极小多项式．设 $\partial^0 g(x)=n_0$，并写

$$g(x)=x^{n_0}+c_1x^{n_0-1}+c_2x^{n_0-2}+\cdots+c_{n_0}$$

$$f(x)=1+c_1x+c_2x^2+\cdots+c_{n_0}x^{n_0},$$

那么根据定理 6，上述自律线性时序线路的任一输出序列都可以由以 $f(x)$ 为联接多项式的 n_0 级线性移位寄存器产生．反过来，可以证明，当 c_1 和 c_2 都不等于 0 时，以 $f(x)$ 为联接多项式的 n_0 级线性移位寄存器从任一初始状态出发所产生的 q 元序列都可以是上述自律线性时序线路自某一初始状态出发产生的输出序列．请读者自己证一下．

例 4 线性移位寄存器的串联．

仍设 $\qquad f_1(x)=1+c_{11}x+c_{12}x^2+\cdots+c_{1n_1}x^{n_1},$

$$c_{1i}\in\mathbf{F}_q,\ i=1,\ 2,\ \cdots,\ n_1,$$

---

* 注意，§1 引理 1 的证明，当 T 奇异时，仍成立．

$$f_2(x)=1+c_{21}x+c_{22}x^2+\cdots+c_{2n_2}x^{n_2},$$
$$c_{2i}\in\mathbf{F}_q,\ i=1,\ 2,\ \cdots,\ n_2.$$
把以 $f_2(x)$ 为联接多项式的 q 元线性移位寄存器串联入以 $f_1(x)$ 为联接多项式的 q 元线性移位寄存器如下:

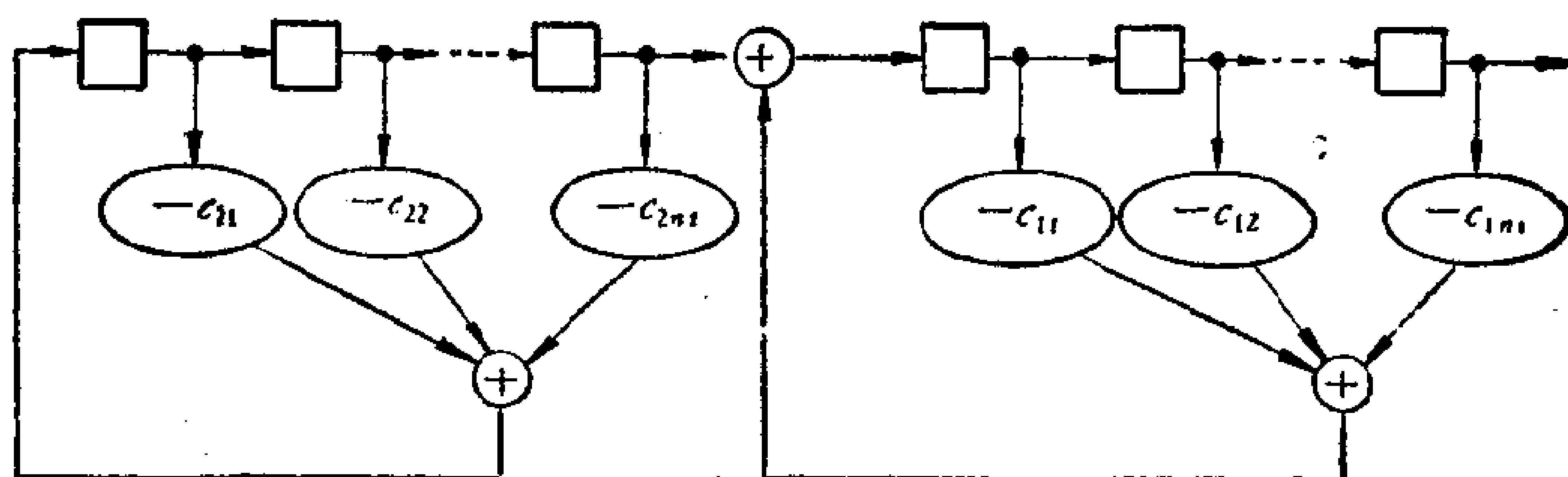


图 12

仍令 $n=n_1+n_2$, 并将图 12 中的自律线性时序线路的 n 个寄存器从右往左依序叫做第 1 个、第 2 个, …, 第 n 个延迟元件. 那么这个自律线性时序线路的状态转移矩阵就是

$$A=\begin{pmatrix} A_1 & 0 \\ E & A_2 \end{pmatrix},$$

其中 E 是 $n_2\times n_1$ 矩阵

$$E=\begin{pmatrix} 0\cdots 0 & 1 \\ \text{\Large 0} & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \end{pmatrix}.$$

令 $\qquad g_i(x)=x^{n_i}+c_{i1}x^{n_i-1}+c_{i2}x^{n_i-2}+\cdots+c_{in_i},\ i=1,\ 2.$

那么 $g_i(x)$ 既是 A_i 的特征多项式, 又是 A_i 的极小多项式. 易证, A 的特征多项式和极小多项式都是 $g_1(x)g_2(x)$.

$$g(x)=g_1(x)g_2(x),$$

那么
$$\partial^0 g(x)=n,$$

设
$$g(x)=x^n+c_1x^{n-1}+c_2x^{n-2}+\cdots+c_n,$$

并令
$$f(x)=1+c_1x+c_2x^2+\cdots+c_nx^n.$$

根据定理 6 可知, 上述自律线性时序线路的任一输出序列都

可以由以 $f(x)$ 为联结多项式的 n 级线性移位寄存器产生. 反之,设

$$a_1, a_2, a_3, \cdots \tag{17}$$

是以 $f(x)$ 为联结多项式的 n 级线性移位寄存器产生的任一 q 元序列对 $k=1, 2, \cdots, n_2$, 将以 $f_1(x)$ 为联接多项式的 n_1 级线性移位寄存器从初始状态 $(a_k, a_{k+1}, \cdots, a_{k+(n_1-1)})$ 出发产生的 q 元序列的第 n_1+1 项记作 b_{n_1+k}.

令 $$c_{n_1+k}=a_{n_1+k}-b_{n_1+k}, k=1, 2, \cdots, n_2.$$

那么上述自律线性时序线路从初始状态

$$\mathbf{s}(0)=(a_1, a_2, \cdots, a_{n_1}, c_{n_1+1}, c_{n_1+2}, \cdots, c_n)$$

出发所产生的输出序列的前 n 项就是(17)的前 n 项. 更因这个输出序列可以由以 $f(x)$ 为联结多项式的 n 级线性移位寄存器产生,所以由它的前 n 项完全确定,因此这个输出序列正好是(17). 上面这两件事实合起来就是说, 把以 $f_2(x)$ 为联结多项式的 n_2 级线性移位寄存器串联入以 $f_1(x)$ 为联接多项式的 n_1 级线性移位寄存器所得的自律线性时序线路与以 $f_1(x)f_2(x)$ 为联接多项式的 n 级线性移位寄存器等效.

例 5 线性移位寄存器的互馈联结*.

考察下面的自律线性时序线路, 它由两个 q 元移位寄存

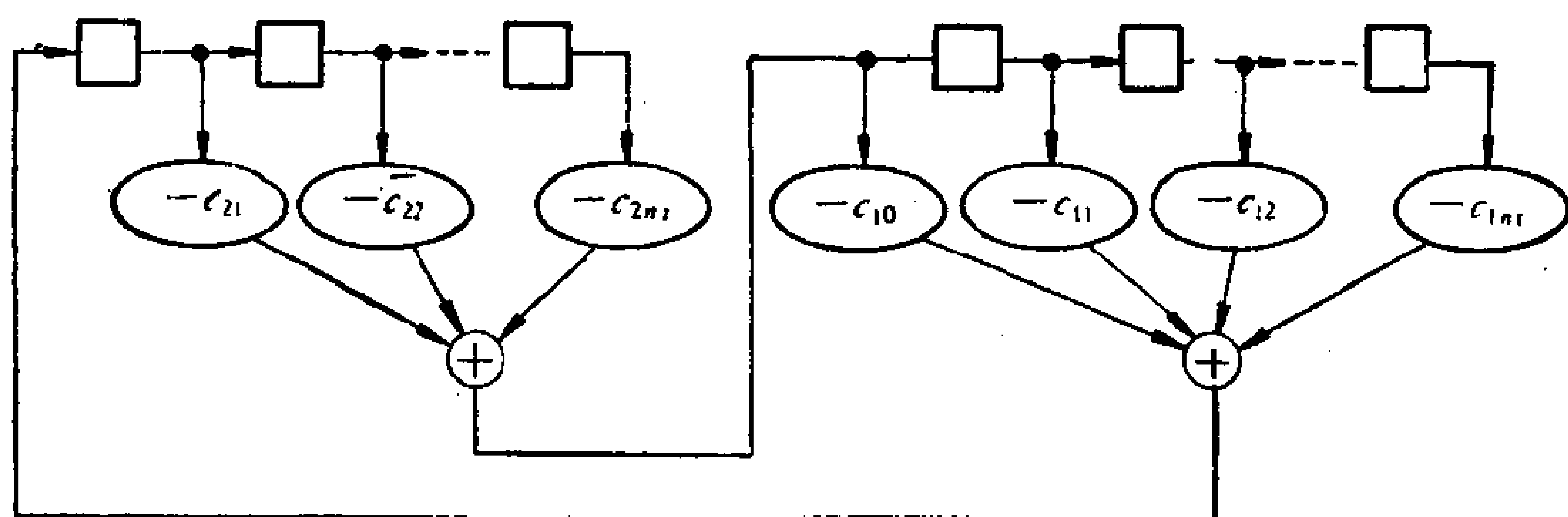


图 13

* 见 Scholefield, P. H. R. Shift Registers Generating Maximum-length Sequences, *Electronic Technology* **37**(1960), 389—394.

器，一个 n_1 级的，另一个 n_2 级的，组合起来的．我们把这种组合方式简称为互馈联接．将这个时序线路的寄存器从右往左依序叫做第 1 个，第 2 个，…，第 n 个，那么这个自律线性时序线路的状态转移矩阵就是

$$A=\begin{pmatrix}
0 & & & & & & & & -c_{1n_1} \\
1 & 0 & & & & & & & \vdots \\
 & 1 & \ddots\ 0 & & & & & & -c_{12} \\
 & & \ddots\ 1 & 0 & & & & & -c_{11} \\
 & & & -c_{2n_2} & 0 & & & & c_{10}c_{2n_2} \\
 & & & \vdots & 1 & 0 & & & \vdots \\
 & & & & & 1 & \ddots\ 0 & & \\
 & & & -c_{22} & & & \ddots & & c_{10}c_{22} \\
 & & & -c_{21} & & & & 1 & c_{10}c_{21}
\end{pmatrix}$$

将 A 的特征多项式 $|xI-A|$ 记作 $g(x)$，经计算可得

$$g(x)=x^n-\sum_{u=0}^{n_1}\sum_{v=1}^{n_2}c_{1u}c_{2v}x^{n-u-v},$$

如果 $g(x)$ 不可约，特别 $g(x)$ 本原，那么 $g(x)$ 也是 A 的极小多项式．这时，根据定理 6，上述自律线性时序线路的任一输出序列都可以由以

$$f(x)=x^n g(1/x)=1-\sum_{u=0}^{n_1}\sum_{v=1}^{n_2}c_{1u}c_{2v}x^{u+v}$$

为联接多项式的 n 级线性移位寄存器经适当选取初态后产生；反之，以 $f(x)$ 为联接多项式的 n 级线性移位寄存器产生的任一序列也可以由上述自律线性时序线路径适当选取初态后产生．

特别，对于 $\mathbf{F}_2$ 上的 n 次本原 5 项式

$$f(x)=1+x^{u+v}+x^{n_1+v}+x^{u+n_2}+x^{n_1+n_2} \tag{18}$$

其中 $n_1+n_2=n$，$0\leqslant u<n_1$，$0<v<n_2$，所产生的 m 序列都可以由将两个线性移位寄存器经互馈联接所得到的图 14 中的那

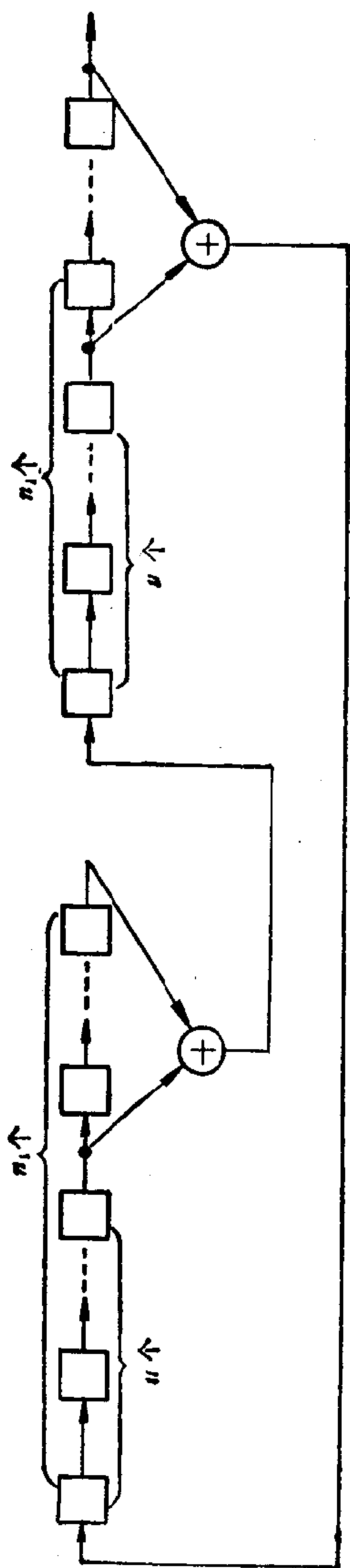


图 14

个自律线性时序线路产生.

图 14 中的线路比直接采用以 (18) 为联接多项式的 n 级线性移位寄存器少用 1 个模 2 加法器. 最后注意, $\mathbf{F}_2$ 上形如

$$x^n+x^{a+b}+x^a+x^b+1,\ 0<a<b<a+b<n$$

的 5 项式的互反多项式

$$1+x^{n-a-b}+x^{n-a}+x^{n-b}+x^n \tag{19}$$

均可写成形状(18); 实际上, 方程组

$$\left.\begin{aligned} u+v&=n-a-b\\ u+n_2&=n-a\\ n_1+v&=n-b\\ n_1+n_2&=n\end{aligned}\right\}$$

总有整数解 n_1, n_2, u, v 而 $n_1>0, n_2>0, 0\leqslant u<n_1, 0<v<n_2$. 下面是形如(19)的本原多项式的例子

$$x^8+x^6+x^5+x+1$$
$$x^{12}+x^7+x^4+x^3+1$$
$$x^{13}+x^4+x^3+x+1$$
$$x^{14}+x^{12}+x^{11}+x+1$$
$$x^{16}+x^5+x^3+x^2+1$$
$$x^{19}+x^6+x^5+x+1$$

例 6　反复寄存器*

J–K 触发器是既有存储功能又有逻辑功能的一种元件, 通常用下面的符号来代表它:

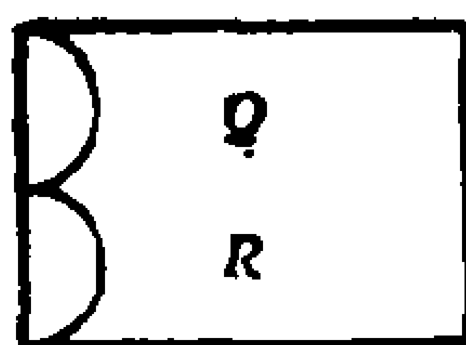


图　15

* 见 Alltop, W. O., Pratt, A. V. and Burton, R. C. Algebraic Theory of Flip-Flop Sequence Generators, *Information and Control* **12** (1968), 193—205.

当 $Q=1$ 时，$R=0$；而当 $Q=0$ 时，$R=1$. 给了两个 J-K 触发器，有下面四种方法把它们串联起来：

i）移位联接. 加一个移位脉冲以后，第一个 J-K 触发器中 Q 和 R 的内容分别移给第二个 J-K 触发器中的 Q 和 R. 这种联接方式表作

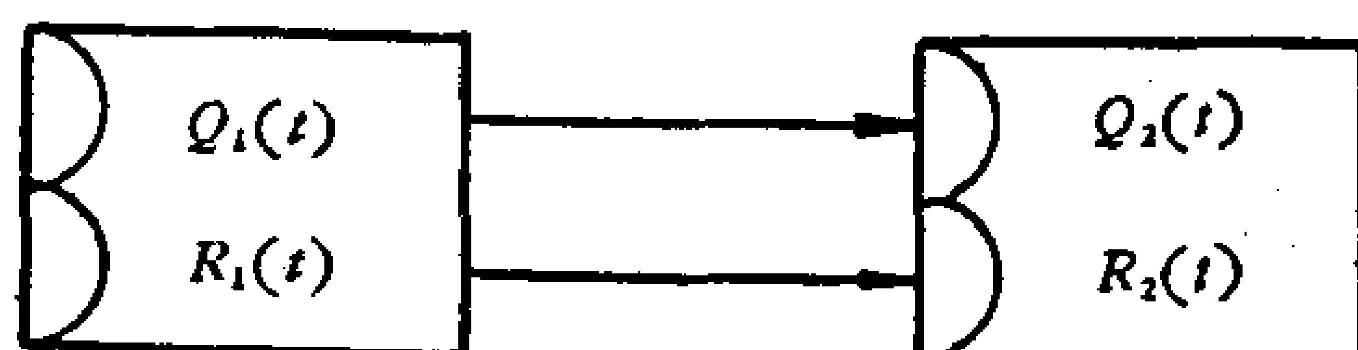


图 16

这时
$$Q_2(t+1)=Q_1(t),$$
$$R_2(t+1)=R_1(t).$$

ii）加 Q 联接. 加一个移位脉冲以后，把第一个 J-K 触发器中 Q 的内容加到第一个 J-K 触发器中 Q 和 R 的内容上. 这种联接方式表作

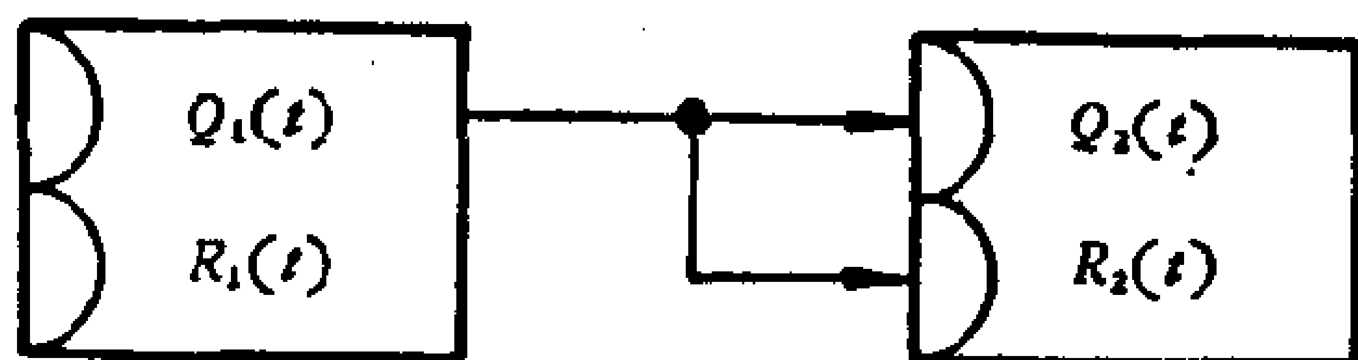


图 17

这时
$$Q_2(t+1)=Q_1(t)+Q_2(t),$$
$$R_2(t+1)=Q_1(t)+R_2(t)=Q_1(t)+Q_2(t)+1.$$

iii）移位并求补联接. 加一个移位脉冲以后，把第一个 J-K 触发器中 Q 和 R 的内容分别移给第二个 J-K 触发器中的 R 和 Q. 这种联接方式表作

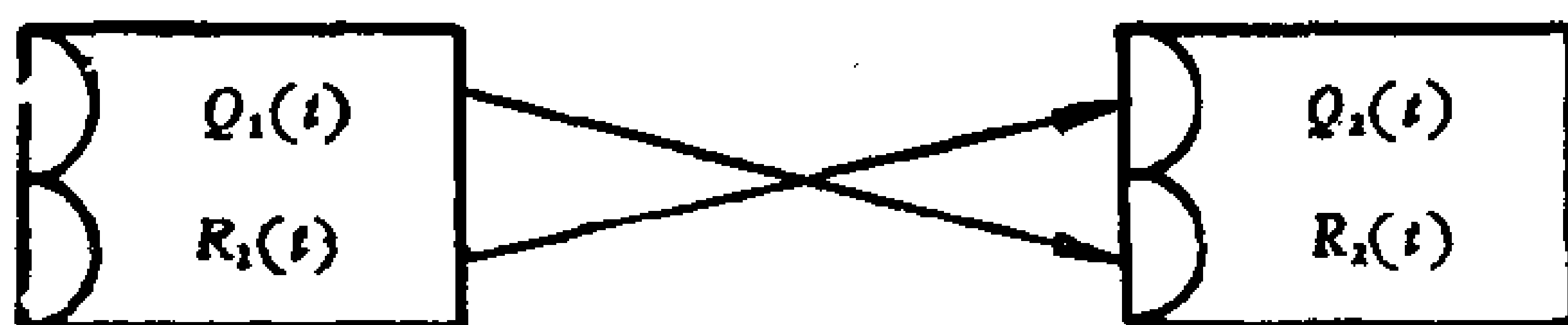


图 18

这时 $$Q_2(t+1)=R_1(t)=Q_1(t)+1,$$
$$R_2(t+1)=Q_1(t)=R_1(t)+1.$$

iv) 加 Q 并求补联接. 加一个移位脉冲以后，把第一个 J-K 触发器中 R 的内容加到第二个 J-K 触发器中 Q 和 R 的内容上. 这种联接方式表作

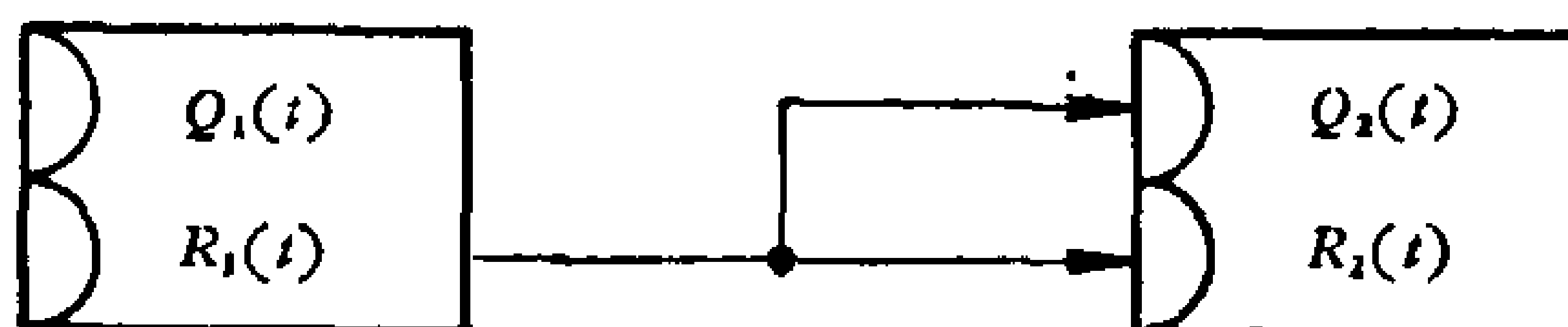


图 19

这时 $$Q_2(t+1)=R_1(t)+Q_2(t)=Q_1(t)+Q_2(t)+1,$$
$$R_2(t+1)=R_1(t)+R_2(t)=Q_1(t)+R_2(t)+1.$$

设有 n 个 J-K 触发器，把第 i 个 J-K 触发器按以上四种方式之一串联入第 $i+1$ 个 J-K 触发器 $(i=1,2,\cdots,n-1)$，当 $i\neq j(1\leqslant i,\ j\leqslant n-1)$ 时，串联的方式不一定相同，同时把第 n 个 J-K 触发器也按以上四种方式之一串联入第 1 个 J-K 触发器. 这样就得到一个 n 级反复寄存器. 例如

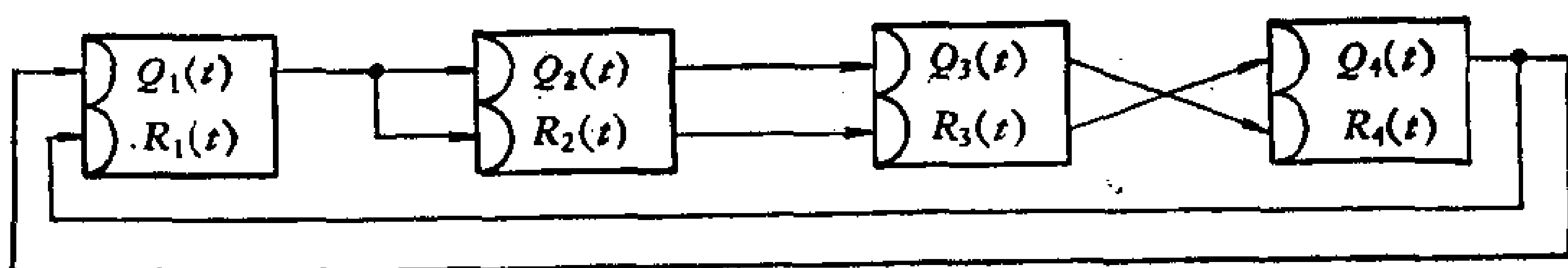


图 20

就是一个 4 级反复寄存器. 因 $R_i(t)$ 总是由 $Q_i(t)$ 唯一确定的: $R_i(t)=Q_i(t)+1$，所以 n 级反复寄存器在时刻 t 的状态就由 n 元组

$$(Q_1(t),\ Q_2(t),\ \cdots,\ Q_n(t))$$

唯一确定. 令

$$T=\begin{pmatrix} t_{11} & 1 & 0 & \cdots & 0 \\ 0 & t_{22} & 1 & \cdots & 0 \\ 0 & 0 & t_{33} & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 1 & 0 & 0 & \cdots & t_{nn} \end{pmatrix}, \tag{20}$$

其中 $t_{ii}=1$，如果把第 $i-1$ 个 J-K 触发器串联入第 i 个 J-K 触发器的方式是加 Q 联接或加 Q 并求补联接；否则 $t_{ii}=0$. 令

$$\mathbf{c}=(c_1,\ c_2,\ \cdots,\ c_n),$$

其中 $c_i=1$，如果把第 $i-1$ 个 J-K 触发器串联入第 i 个 J-K 触发器的方式是移位并求补联接或加 Q 并求补联接；否则 $c_i=0$. 那么这个反复寄存器的状态转移变换就是

$$\begin{aligned}&(Q_1(t+1),\ Q_2(t+1),\ \cdots,\ Q_n(t+1))\\&\quad=(Q_1(t),\ Q_2(t),\ \cdots,\ Q_n(t))T+\mathbf{c},\end{aligned} \tag{21}$$

我们把这个变换记作 $A_{T,\mathbf{c}}$. 也可以定义以 $A_{T,\mathbf{c}}$ 为状态转移变换的反复寄存器的状态图，它是一个有向图，顶点集是 $V_n(\mathbf{F}_2)$，而弧集是

$$\{((a_1,\ a_2,\ \cdots,\ a_n),\ (a_1,\ a_2,\ \cdots,\ a_n)A_{T,\mathbf{c}}) \\ \times \mid (a_1,\ a_2,\ \cdots,\ a_n)\in V_n(\mathbf{F}_2)\}.$$

引理 3 $|T|\neq 0$，当且仅当至少有一个 $t_{ii}=0(1\leqslant i\leqslant n)$. 如果 $t_{11}=t_{22}=\cdots=t_{nn}=1$，那么 T 的秩等于 $n-1$.

证. 利用第二章 §5 行列式的性质 6，可得

$$|T|=t_{11}t_{22}\cdots t_{nn}+1$$

因此 $|T|\neq 0$，当且仅当 $t_{11}t_{22}\cdots t_{nn}=0$，即至少有一个 $t_{ii}=0$. 当 $t_{11}=t_{22}=\cdots=t_{nn}=1$ 时，$|T|=0$，但 T 的前 $n-1$ 行线性无关，因此 T 的秩等于 $n-1$.

现在设 T 是 $\mathbf{F}_2$ 上的任意 $n\times n$ 矩阵，而 $\mathbf{c}$ 是 $V_n(\mathbf{F}_2)$ 中

任一向量. 我们把作用在 $V_n(\mathbf{F}_2)$ 上的变换

$$(a_1, a_2, \cdots, a_n) \to (a_1, a_2, \cdots, a_n)T + \mathbf{c} \qquad (22)$$

叫做一个广义仿射变换. 例如, 上面讨论的 n 级反复寄存器的状态转移变换(21)就是广义仿射变换. 注意, 当 $\mathbf{c} \neq \mathbf{0}$ 时, 广义仿射变换(22)并不是向量空间 $V_n(\mathbf{F}_2)$ 的线性变换; 但当 $\mathbf{c} = \mathbf{0}$ 时, 它是线性变换. 如果广义仿射变换 (22) 中的 $n \times n$ 矩阵 T 是非异矩阵,(22)就叫一个仿射变换.

两个广义仿射变换 $A_{T_1, \mathbf{c}_1}$ 和 $A_{T_2, \mathbf{c}_2}$ 的乘积, 定义为先作用 $A_{T_1, \mathbf{c}_1}$, 然后再作用 $A_{T_2, \mathbf{c}_2}$ 的变换, 记作 $A_{T_1, \mathbf{c}_1} \cdot A_{T_2, \mathbf{c}_2}$. 显然有

$$A_{T_1, \mathbf{c}_1} \cdot A_{T_2, \mathbf{c}_2} = A_{T_1 T_2, \mathbf{c}_1 T_2 + \mathbf{c}_2}$$

对于这样定义的乘法, 广义仿射变换 $A_{T, \mathbf{c}}$ 有逆, 当且仅当它是仿射变换, 即 $|T| \neq 0$; 当 $|T| \neq 0$ 时, $A_{T, \mathbf{c}}$ 的逆

$$A_{T, \mathbf{c}}^{-1} = A_{T^{-1}, \mathbf{c}T^{-1}}.$$

两个广义仿射变换 $A_{T_1, \mathbf{c}_1}$ 和 $A_{T_2, \mathbf{c}_2}$ 叫相似, 如果有一个仿射变换 $A_{P, \mathbf{y}}$, 使

$$A_{T_2, \mathbf{c}_2} = A_{P, \mathbf{y}}^{-1} A_{T_1, \mathbf{c}_1} A_{P, \mathbf{y}}.$$

同样可以定义广义仿射变换 $A_{T, \mathbf{c}}$ 的图, 它的顶点集是 $V_n(\mathbf{F}_2)$, 而弧集是 $\{(\mathbf{a}, \mathbf{a}T + \mathbf{c}) \mid \mathbf{a} \in V_n(\mathbf{F}_2)\}$.

引理 4 两个相似的广义仿射变换的图一定同构.

我们把这个引理的证明留给读者去作.

引理 5 用 u 表 n 级反复寄存器中加 Q 联接与加 Q 并求补联接的个数, 即 $t_{ii} = 1$ 的个数. 那么 $A_{T, \mathbf{c}}$ 与一线性变换相似, 当且仅当 $0 < u \leqslant n$ 或 $u = 0$ 而 $\mathbf{c}$ 的不等于 0 的分量的个数, 记作 $w(\mathbf{c})$, 是偶数. 当这两个条件之一成立时, $A_{T, \mathbf{c}}$ 与 $A_{T, \mathbf{0}}$ 相似.

证. 假设有仿射变换 $A_{P, \mathbf{y}}$ 使

$$A_{P, \mathbf{y}}^{-1} A_{T, \mathbf{c}} A_{P, \mathbf{y}} = A_{T_1, \mathbf{0}}.$$

那么

$$P^{-1}TP=T_1,\quad (\mathbf{y}P^{-1}T+\mathbf{c})P+\mathbf{y}=0.$$

从后面的方程得

$$\mathbf{y}P^{-1}(T+I)+\mathbf{c}=\mathbf{0}.$$

易证上面这个方程有解，当且仅当 $u>0$ 或 $u=0$ 而 $w(\mathbf{c})$ 是偶数. 当 $u>0$ 或 $u=0$ 而 $w(\mathbf{c})$ 是偶数时，取 $P=I$，$\mathbf{y}(T+I)+\mathbf{c}=0$ 仍有解. 因此这时 $A_{T,\mathbf{c}}$ 与 $A_{T,\mathbf{0}}$ 相似：

当 $u>0$ 或 $u=0$ 而 $\omega(\mathbf{c})$ 是偶数时，要研究 $A_{T,\mathbf{c}}$ 的图，只要研究线性变换 $A_{T,\mathbf{0}}$ 的图，即 T 的图 G_T 就行了. 根据定理 1，G_T 由 T 的初等因子组完全确定.

引理 6 仍设 u 是 n 级反复寄存器中加 Q 联结与加 Q 并求补联接的个数. 那么 T 的特征多项式和极小多项式都等于

$$x^{n-u}(x+1)^u+1.$$

证. 我们有

$$xI-T=\begin{pmatrix} x+t_{11} & 1 & & & \\ & x+t_{22} & 1 & & \\ & & x+t_{33} & \ddots & \\ & & & \ddots & 1 \\ 1 & & & & x+t_{nn} \end{pmatrix}.$$

用初等变换来求 $xI-T$ 的不变因子. 交换头两列，然后将第 2 列加上第 1 列的 $x+t_{11}$ 倍，再将第 2 行加上第 1 行的 $x+t_{22}$ 倍，得

$$\begin{pmatrix} 1 & 0 & & & & \\ & \prod_{i=1}^{2}(x+t_{ii}) & 1 & & & \\ & & x+t_{33} & \ddots & & \\ & & & \ddots & \ddots & 1 \\ & & & & \ddots & \\ 0 & 1 & 0 & \cdots & 0 & x+t_{nn} \end{pmatrix}.$$

交换上面这个矩阵的第 2 列和第 3 列，然后将第 3 列加上第 2 列的 $\prod_{i=1}^{2}(x+t_{ii})$ 倍，再将第 3 行加上第 2 行的 $x+t_{33}$ 倍，得

$$\begin{pmatrix} 1 & 0 & & & & & \\ & 1 & 0 & & & & \\ & & \prod_{i=1}^{3}(x+t_{ii}) & 1 & & & \\ & & & \ddots & \ddots & & \\ & & & x+t_{44} & \ddots & \ddots & \\ & & & & \ddots & \ddots & 1 \\ 0 & 0 & 1 & 0 & \cdots & 0 & x+t_{nn} \end{pmatrix}.$$

如此继续下去，最后将 $xI-T$ 化成

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 & \\ & & & & \prod_{i=1}^{n}(x+t_{ii})+1 \end{pmatrix}.$$

因此 T 的特征多项式和极小多项式都等于

$$\prod_{i=1}^{n}(x+t_{ii})+1=x^{n-u}(x+1)^u+1.$$

当 $u>0$ 或 $u=0$ 而 $w(\mathbf{c})$ 是偶数时，要研究 $A_{T,\mathbf{c}}$ 的图，只要将 $x^{n-u}(x+1)^u+1$ 分解成两两不同的不可约多项式的幂的乘积就行了．这些两两不同的不可约多项式的幂就是 T 的初等因子组，它们完全确定了 T 的图，也即 $A_{T,\mathbf{c}}$ 的图．

当 $u=0$ 而 $w(\mathbf{c})$ 是偶数时，$A_{T,\mathbf{c}}$ 不和线性变换相似．但这时可以用 $(n+1)\times(n+1)$ 矩阵

$$\begin{pmatrix} T & \\ \mathbf{c} & 1 \end{pmatrix}$$

来代表 $A_{T,\mathbf{c}}$．我们把这个矩阵也记作 $A_{T,\mathbf{c}}$，并把 n 级反复寄

存器的状态集取作

$$\{(a_1, a_2, \cdots, a_n, 1) | a_1, a_2, \cdots, a_n \in \mathbf{F}_2\},$$

那么这个 n 级反复寄存器的状态图就是 $(n+1)\times(n+1)$ 矩阵 $A_{T,\mathbf{c}}$ 的图的一个子图. 因这时 T 非异, 所以 $A_{T,\mathbf{c}}$ 也非异. 因此 $A_{T,\mathbf{c}}$ 的图由一些圈组成, 于是这个 n 级反复寄存器的图也由一些圈组成. 从引理 6 可以推出

引理 7 当 $u=0$ 而 $w(\mathbf{c})$ 是奇数时,

$$A_{T,\mathbf{c}}=\begin{pmatrix} T & \\ \mathbf{c} & 1 \end{pmatrix}$$

的特征多项式和极小多项式都等于 $(x+1)(x^n+1)$.

不难证明 $(x+1)(x^n+1)$ 的周期等于 $2n$. 因此当 $u=0$ 而 $w(\mathbf{c})$ 是奇数时, 这个 n 级反复寄存器的状态图中圈的周期都是 $2n$ 的因数.

综合上面这几个引理, 我们有

定理 7 用 u 表 n 级反复寄存器中加 Q 联接和加 Q 并求补联接的个数, 用 w 表示它的移位求补联接和加 Q 并求补联接的个数. 那么当 $0<u\leqslant n$ 或 $u=0$ 而 w 是偶数时, 这个反复寄存器的状态图和以 $x^{n-u}(x+1)^u+1$ 既为特征多项式又为极小多项式的 $n\times n$ 矩阵(20)的状态图同构. 当 $u=0$ 而 w 是奇数, 这个反复寄存器的状态图由一些圈长等于 $2n$ 的因数的圈组成.

将 $x^{n-u}(x+1)^u+1$ 记作 $g_{n,u}(x)$, 并将它写作

$$g_{n,u}(x)=x^{n-u}(x+1)^u+1=x^n+c_1x^{n-1}+c_2x^{n-2}+\cdots+c_n.$$

再令 $f_{n,u}(x)=x^n g_{n,u}(1/x)=1+c_1x+c_2x^2+\cdots+c_nx^n$.

我们还有

定理 8 假定一个 n 级反复寄存器中 J-K 触发器之间的联接方式只有加 Q 联接和移位联接, 并用 u 来代表加 Q 联

接的个数. 那么这个反复寄存器从任一初始状态 $(Q_1(0), Q_2(0), \cdots, Q_n(0))$ 出发，产生的 n 个二元序列

$$Q_i(0),\ Q_i(1),\ Q_i(2),\ \cdots,\ i=1,\ 2,\ \cdots,\ n,$$

都适合递归关系式

$$Q_i(k)=c_1Q_i(k-1)+c_2Q_i(k-2)+\cdots+c_nQ_i(k-n),\ k\geqslant n, \tag{23}$$

即都可以由以 $f_{n,u}(x)$ 为联接多项式的 n 级线性移位寄存器产生. 反过来，设

$$a_0,\ a_1,\ a_2,\ \cdots \tag{24}$$

是由以 $f_{n,u}(x)$ 为联接多项式的 n 级线性移位寄存器产生的任一二元序列，那么总可适当选择反复寄存器的初态，使

$$a_t=Q_n(t),\ t=0,\ 1,\ 2,\ \cdots.$$

证. 第一个断言是定理6的第一个断言的特例. 因此只要证明第二个断言. 设(24)适合递归关系式

$$a_k=c_1a_{k-1}+c_2a_{k-2}+\cdots+c_na_{k-n},\ k\geqslant n. \tag{25}$$

用归纳法依次选定 $Q_n(0), Q_{n-1}(0), \cdots, Q_1(0)$. 首先选

$$Q_n(0)=a_0.$$

当 $Q_n(0), Q_{n-1}(0), \cdots, Q_i(0)(n\geqslant i>1)$ 已选定后，令

$$Q_{i-1}(0)=Q_i(0)t_{ii}+a_{n-i+1}.$$

那么这个反复寄存器，从初始状态 $(Q_1(0), Q_2(0), \cdots, Q_n(0))$ 出发，第 n 个 J-K 触发器输出的二元序列的前 n 项就是

$$Q_n(0)=a_0,\ Q_n(1)=a_1,\ \cdots,\ Q_n(n-1)=a_{n-1}.$$

但(24)和

$$Q_n(0),\ Q_n(1),\ Q_n(2),\ \cdots$$

都适合同一 n 级线性递归关系式(23)，也即(25)，因此一定有

$$a_t=Q_n(t),\ t=0,\ 1,\ 2,\ \cdots.$$

最后，我们指出，Alltop, W. O., Pratt, A. V. 和

Burton, R. C. 编了一个 $x^{n-u}(x+1)^u+1$ 的完全因式分解表*，其中 $2\leqslant n\leqslant 19$ 而 $0\leqslant u\leqslant n$. 这个表表明，当 n 和 u 取以下这些值时：

表 1

n	2	3	4	5	6	7	9	10	11	15	17	18
μ	1	1,2	1	2,3	1,5	1,3,4,6	4,5	7	2,9	1,4,8,11	3,5,6,11,12,14	11

$x^{n-u}(x+1)^u+1$ 是本原多项式. 因此当 $n=2, 3, 4, 5, 6, 7, 9, 10, 11, 15, 17, 18$ 时，可以利用反复寄存器来产生 m 序列.

§ 11 q 元周期序列的几种表示法

在这一节里我们要介绍 q 元周期序列的几种表示法，即形式幂级数表示法，有理分式表示法和根表示法. 这几种表示法是讨论 q 元周期序列的有力工具. 我们将利用它们重新导出前几节的某些结论.

我们先从形式幂级数表示法开始. 设

$$\mathbf{a}=(a_0, a_1, a_2, \cdots), a_i\in \mathbf{F}_q \tag{1}$$

是一个 q 元周期序列. 让它相应一个幂级数

$$a_0+a_1x+a_2x^2+\cdots,$$

其中 x 是一个符号(或文字)，称为它的*形式幂级数表示*. 对这种幂级数我们并不考虑它的收敛性，但仍可仿照数学分析中一样对它进行形式的代数运算，因而把它叫做形式幂级数. 通过这些形式的代数运算有时可以得出形式幂级数的一些性质，而这些性质自然反映了它所相应的 q 元周期序列的性质.

设 $\mathbf{F}_q$ 是 q 个元素的有限域，而 x 是一个符号（或称文

* 见第 379 页脚注中所列资料.

字）．形如

$$a_0+a_1x+a_2x^2+\cdots,\ a_i\in\mathbf{F}_q \tag{2}$$

的式子叫做系数属于 $\mathbf{F}_q$ 的（符号）x 的形式幂级数．a_0, a_1, a_2, … 叫做这个形式幂级数的系数，特别 a_i 叫做它的 i 次项 a_ix^i 的系数．a_0, a_1, a_2, …之中可以有无限多个不等于 0，当它们之中只有有限个不等于 0 时，(2) 就是 x 的多项式．因此 x 的多项式可以看作是 x 的形式幂级数的特例．我们往往把形式幂级数 (2) 简记作

$$\sum_{i=0}^{\infty} a_ix^i \tag{3}$$

我们有时也用 $f(x)$, $g(x)$, …来表示 x 的形式幂级数．我们把 $\mathbf{F}_q$ 上 x 的形式幂级数的全体所组成的集合记作 $\mathbf{F}_q[[x]]$.

设

$$\sum_{i=0}^{\infty} b_ix^i,\ b_i\in\mathbf{F}_q, \tag{4}$$

也是一个形式幂级数．如果 (3) 和 (4) 的同次项的系数都相等，即 $a_i=b_i(i=0, 1, 2, \cdots)$，我们就说 (2) 和 (3) 相等，记作

$$\sum_{i=0}^{\infty} a_ix^i=\sum_{i=0}^{\infty} b_ix^i.$$

我们来规定 $\mathbf{F}_q[[x]]$ 中的加法运算和乘法运算．设

$$f(x)=\sum_{i=0}^{\infty} a_ix^i,\ g(x)=\sum_{i=0}^{\infty} b_ix^i$$

是 $\mathbf{F}_q$ 上 x 的两个形式幂级数．我们用下面的式子来规定 $f(x)$ 与 $g(x)$ 的和与积：

$$\sum_{i=0}^{\infty} a_ix^i+\sum_{i=0}^{\infty} b_ix^i=\sum_{i=0}^{\infty} (a_i+b_i)x^i,$$

$$\sum_{i=0}^{\infty} a_ix^i\cdot\sum_{i=0}^{\infty} b_ix^i=\sum_{i=0}^{\infty}\Big(\sum_{k=0}^{i} a_kb_{i-k}\Big)x^i.$$

那么容易验证 $\mathbf{F}_q[[x]]$ 对于这样规定的加法运算和乘法运算组成一个无零因子的交换环，叫做 $\mathbf{F}_q$ 上符号 x 的形式幂级数

环. 这个环的零元素是

$$0=\sum_{i=0}^{\infty}0x^i,$$

单位元素是

$$1=1+\sum_{i=0}^{\infty}0x^i,$$

而(3)的负元素是

$$\sum_{i=0}^{\infty}(-a_i)x^i.$$

$\mathbf{F}_q[[x]]$ 中的非零元素并不一定是可逆的. 一个元素是可逆的充要条件由下面的定理给出

定理 1 $\mathbf{F}_q$ 上 x 的形式幂级数 $\sum_{i=0}^{\infty}a_ix^i$ 是可逆的,当且仅当 $a_0\neq 0$.

证. 先设 $\sum_{i=0}^{\infty}a_ix^i$ 是可逆的,并设它的逆是 $\sum_{i=0}^{\infty}b_ix^i$, 即

$$\sum_{i=0}^{\infty}a_ix^i\cdot\sum_{i=0}^{\infty}b_ix^i=1 \tag{5}$$

比较上式双方的零次项得 $a_0b_0=1$, 因此 $a_0\neq 0$.

反之,设 $a_0\neq 0$. 比较 (5) 式双方同幂次的各项的系数得

$$\begin{aligned}
&a_0b_0=1,\\
&a_0b_1+a_1b_0=0,\\
&a_0b_2+a_1b_1+a_2b_0=0,\\
&\cdots\cdots\cdots\cdots\\
&a_0b_n+a_1b_{n-1}+\cdots+a_nb_1=0,\\
&\cdots\cdots\cdots\cdots.
\end{aligned}$$

由第一式解出 b_0, 接着又由第二式解出 b_1, 再接着又由第三式解出 b_2, 如此下去就唯一地定出了 $\sum_{i=0}^{\infty}a_ix^i$ 的逆 $\sum_{i=0}^{\infty}b_ix^i$.

这证明了定理 1.

当 $a_0\neq 0$ 时,我们往往用

$$\frac{1}{\sum_{i=0}^{\infty} a_i x^i}$$

来代表$\sum_{i=0}^{\infty} a_i x^i$的逆，并用

$$\sum_{i=0}^{\infty} b_i x^i \Big/ \sum_{i=0}^{\infty} a_i x^i$$

来代表$\sum_{i=0}^{\infty} b_i x^i$与$\sum_{i=0}^{\infty} a_i x^i$的逆的乘积.

根据定理1,

$$1+x+x^2+\cdots \tag{6}$$

是可逆的. 容易验证

$$(1+x+x^2+\cdots)(1-x)=1,$$

即$1-x$是(6)的逆，或者说(6)是$1-x$的逆. 因此可以写

$$\frac{1}{1-x}=1+x+x^2+\cdots.$$

同理，对任一正整数l，有

$$\frac{1}{1-x^l}=1+x^l+x^{2l}+\cdots.$$

设$\sum_{i=0}^{\infty} a_i x^i$和$\sum_{i=0}^{\infty} b_i x^i$是两个形式幂级数，如果有形式幂级数$\sum_{i=0}^{\infty} c_i x^i$存在，使

$$\sum_{i=0}^{\infty} b_i x^i=\sum_{i=0}^{\infty} c_i x^i \cdot \sum_{i=0}^{\infty} a_i x^i,$$

我们就说$\sum_{i=0}^{\infty} a_i x^i$除得尽$\sum_{i=0}^{\infty} b_i x^i$，而商是$\sum_{i=0}^{\infty} c_i x^i$. 这时我们记

$$\sum_{i=0}^{\infty} b_i x^i \Big/ \sum_{i=0}^{\infty} a_i x^i=\sum_{i=0}^{\infty} c_i x^i.$$

如果$a_0=a_1=\cdots=a_n=0$而$a_{n+1}\neq 0$，那么仿照定理1可证：$\sum_{i=0}^{\infty} a_i x^i$除得尽$\sum_{i=0}^{\infty} b_i x^i$，当且仅当$b_0=b_1=\cdots=b_n=0$.

我们曾经定义过作用在 q 元序列(1)上的左移变换 L:

$$L(\mathbf{a})=(a_1,\ a_2,\ \cdots).$$

显然,相应于 $L(\mathbf{a})$ 的形式幂级数是

$$\sum_{i=1}^{\infty} a_i x^{i-1}=\frac{\sum_{i=0}^{\infty} a_i x^i-a_0}{x},$$

而相应于 $L^t(\mathbf{a})$ 的形式幂级数是

$$\frac{\sum_{i=0}^{\infty} a_i x^i-\sum_{i=0}^{t-1} a_i x^i}{x^t}.$$

类似地,我们可以定义作用在 q 元序列(1)上的右移变换 R:

$$R(\mathbf{a})=(0,\ a_0,\ a_1,\ a_2,\ \cdots),$$

那么相应于 $R^t(\mathbf{a})$ 的形式幂级数是

$$x^t\cdot\sum_{i=0}^{\infty} a_i x^i,$$

即将 $\mathbf{a}$ 右移 t 位,相应的形式幂级数就要乘以 x^t. 注意,相应于 $R^tL^t(\mathbf{a})$ 的形式幂级数是

$$\sum_{i=0}^{\infty} a_i x^i-\sum_{i=0}^{t-1} a_i x^i,$$

即它由相应于 $\mathbf{a}$ 的形式幂级数减去前 t 项而得.

我们先给出一个 q 元序列是周期序列的充要条件.

定理2 设

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),\ \ a_i\in\mathbf{F}_q \tag{1}$$

是一个 q 元序列,而

$$\sum_{i=0}^{\infty} a_i x^i \tag{3}$$

是它的形式幂级数表示. 那么 $\mathbf{a}$ 是周期序列, 当且仅当可将(3)表成一个有理分式,其中分子的次数小于分母的次数而分母的零次项等于1.

证. 先设 $\mathbf{a}$ 是周期序列,而它的周期等于 l. 那么

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}$$
$$+ a_0 x^l + a_1 x^{l+1} + a_2 x^{l+2} + \cdots + a_{l-1} x^{2l-1}$$
$$+ a_0 x^{2l} + a_1 x^{2l+1} + a_2 x^{2l+2} + \cdots + a_{l-1} x^{3l-1} + \cdots$$
$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}$$
$$+ (a_0 + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}) x^l$$
$$+ (a_0 + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}) x^{2l} + \cdots$$
$$= (a_0 + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1})(1 + x^l + x^{2l} + \cdots)$$
$$= \frac{a_0 + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}}{1 - x^l}.$$

最后这个式子是个有理分式，它的分子的次数小于分母的次数，而分母的零次项等于 1.

再设(3)可以表成

$$\sum_{i=0}^{\infty} a_i x^i = \frac{g(x)}{f(x)},$$

其中 $f(x)$, $g(x) \in \mathbf{F}_q[x]$, $\partial^0 g(x) < \partial^0 f(x)$, 而 $f(x)$ 的零次项等于 1. 我们定义 $f(x)$ 的周期为元素 x 在交换群 $\mathbf{F}_q[x]^*_{f(x)}$ 中的阶. 因为 $\mathbf{F}_q[x]^*_{f(x)}$ 是个有限群，所以 $f(x)$ 的周期是个正整数，设为 l. 那么有 $d(x) \in \mathbf{F}_q[x]$ 使

$$1 - x^l = f(x) d(x).$$

于是
$$\frac{g(x)}{f(x)} = \frac{g(x) d(x)}{f(x) d(x)} = \frac{h(x)}{1 - x^l},$$

其中 $h(x) = g(x) d(x)$. 显然 $\partial^0 h(x) < l$. 写

$$h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{l-1} x^{l-1},$$

那么
$$\sum_{i=0}^{\infty} a_i x^i = \frac{g(x)}{f(x)} = \frac{h(x)}{1 - x^l} = h(x)(1 + x^l + x^{2l} + \cdots)$$
$$= h(x) + h(x) x^l + h(x) x^{2l} + \cdots.$$

由此推出

$$a_{\lambda l + k} = h_k,\ k = 0, 1, 2, \cdots, l-1;\ \lambda = 0, 1, 2, \cdots.$$

这证明了(1)是周期序列.

如果 q 元周期序列 $\mathbf{a}$ 的形式幂级数表示可以表成有理分式

$$\sum_{i=0}^{\infty} a_i x^i = \frac{g(x)}{f(x)},$$

其中 $f(x),\ g(x)\in \mathbf{F}_q[x]$, $\partial^0 g(x)<\partial^0 f(x)$, 而 $f(x)$ 的零次项等于1, 我们就说 $\frac{g(x)}{f(x)}$ 是 q 元周期序列 $\mathbf{a}$ 的一个有理分式表示, 也说 $f(x)$ 是 $\mathbf{a}$ 的一个生成多项式. 下面的定理指明 q 元周期序列的有理分式表示与产生它的线性移位寄存器的关系.

定理 3 设 $\frac{g(x)}{f(x)}$ 是 q 元周期序列 $\mathbf{a}$ 的一个有理分式表示, 那么 $f(x)$ 是产生 $\mathbf{a}$ 的一个线性移位寄存器的联接多项式. 反过来, 如果 $f(x)$ 是产生 $\mathbf{a}$ 的一个线性移位寄存器的联接多项式, 那么 $\mathbf{a}$ 有一个有理分式表示以 $f(x)$ 为分母.

证. 设 $\frac{g(x)}{f(x)}$ 是 q 元周期序列 $\mathbf{a}$ 的一个有理分式表示, 即

$$\sum_{i=0}^{\infty} a_i x^i = \frac{g(x)}{f(x)}, \tag{7}$$

其中 $f(x),\ g(x)\in \mathbf{F}_q[x]$, $\partial^0 g(x)<\partial^0 f(x)$, 而 $f(x)$ 的零次项等于1. 令

$$f(x)=1+c_1x+c_2x^2+\cdots+c_nx^n,\ c_n\neq 0,$$
$$g(x)=b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1}.$$

那么由(7)式推出

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\cdot(1+c_1x+c_2x^2+\cdots+c_nx^n)$$
$$=b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1}.$$

比较双方同次项的系数得到

$$\begin{pmatrix} 1 & & & & \\ c_1 & 1 & & & \\ c_2 & c_1 & 1 & & \\ \vdots & \ddots & \ddots & \ddots & \\ c_n & \cdots\cdots c_2 & c_1 & & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{pmatrix} \tag{8}$$

$$a_{n+k} = -(c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_n a_k), \quad k=0, 1, 2, \cdots \tag{9}$$

由(9)可知，**a** 是以 $f(x)$ 为联接多项式的 n 级线性移位寄存器从初始状态 $(a_0, a_1, a_2, \cdots, a_{n-1})$ 出发所产生的线性移位寄存器序列.

反过来，设

$$f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_n x^n, \ c_n \neq 0$$

是产生 **a** 的一个 n 级线性移位寄存器的联接多项式. 那么由(8)可解出 $b_0, b_1, b_2, \cdots, b_{n-1}$. 令

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1}.$$

不难验证
$$\sum_{i=0}^{\infty} a_i x^i = \frac{g(x)}{f(x)},$$

即 **a** 有一个有理分式表示，其分母是 $f(x)$.

设 $f(x)$ 是 $\mathbf{F}_q$ 上零次项等于 1 的一个 n 次多项式. 用 $G(f)$ 表以 $f(x)$ 为联接多项式的 n 级线性移位寄存器所产生的所有移位寄存器序列的集合. 再用 $\widetilde{G}(f)$ 表示 $G(f)$ 中序列的形式幂级数表示的集合. 我们有

系理 设 $f(x)$ 是 $\mathbf{F}_q$ 上零次项等于 1 的一个多项式. 那么

$$\widetilde{G}(f) = \left\{ \frac{g(x)}{f(x)} \middle| g(x) \in \mathbf{F}_q[x], \ \partial^0 g(x) < \partial^0 f(x) \right\}$$

定理 4 设 $\dfrac{g(x)}{f(x)}$ 是 q 元周期序列 **a** 的一个有理分式表示，而 $(f(x), g(x)) = 1$，那么 $f(x)$ 是产生 **a** 的任一线性移

位寄存器的联接多项式的因式，因而是唯一确定的. 反过来，如果$f(x)$是产生$\mathbf{a}$的线性移位寄存器的联接多项式中次数最低的一个，那么在$\mathbf{a}$的有理分式表示$\frac{g(x)}{f(x)}$中，$(f(x), g(x))=1$.

证. 设$\frac{g(x)}{f(x)}$是q元周期序列$\mathbf{a}$的一个有理分式表示，而$(f(x), g(x))=1$. 再设$f_1(x)$是产生$\mathbf{a}$的任意一个线性移位寄存器的联接多项式，那么根据定理3，$\mathbf{a}$有一个有理分式表示以$f_1(x)$为分母；设这个有理分式表示是$\frac{g_1(x)}{f_1(x)}$. 那么由

$$\sum_{i=0}^{\infty} a_i x^i = \frac{g(x)}{f(x)} \text{ 和 } \sum_{i=0}^{\infty} a_i x^i = \frac{g_1(x)}{f_1(x)}$$

推出
$$\frac{g(x)}{f(x)} = \frac{g_1(x)}{f_1(x)},$$

$$f_1(x)g(x) = f(x)g_1(x).$$

因$(f(x), g(x))=1$，由唯一因式分解定理（即第一章§2定理3）推出

$$f(x) \mid f_1(x).$$

反过来，设$f(x)$是产生q元周期序列$\mathbf{a}$的线性移位寄存器的联接多项式中次数最低的一个. 那么$\mathbf{a}$有有理分式表示$\frac{g(x)}{f(x)}$. 如果有$d(x)\in \mathbf{F}_q[x]$而$d(x)\mid f(x)$, $d(x)\mid g(x)$，不妨设$d(x)$的零次项等于1，并令

$$f(x)=d(x)f_1(x),\ g(x)=d(x)g_1(x),$$

其中$f_1(x), g_1(x)\in \mathbf{F}_q[x]$. 那么

$$\sum_{i=0}^{\infty} a_i x^i = \frac{g(x)}{f(x)} = \frac{g_1(x)}{f_1(x)},$$

$f_1(x)$的零次项等于1而

$$\partial^0 g_1(x)=\partial^0 g(x)-\partial^0 d(x)<\partial^0 f(x)-\partial^0 d(x)=\partial^0 f_1(x).$$

因此 $\frac{g_1(x)}{f_1(x)}$ 也是 $\mathbf{a}$ 的一个有理分式表示. 根据定理 3, $f_1(x)$ 也是产生 $\mathbf{a}$ 的一个线性移位寄存器的联接多项式. 因 $f(x)$ 是产生 $\mathbf{a}$ 的线性移位寄存器的联接多项式中次数最低的一个，所以 $d(x)=1$. 这证明了 $(f(x), g(x))=1$.

根据定理 4 我们知道，产生 q 元周期序列 $\mathbf{a}$ 的最短线性移位寄存器是唯一确定的，因而它的联接多项式也是唯一确定的. 我们把产生 $\mathbf{a}$ 的最短线性移位寄存器的联接多项式叫做它的极小多项式. 我们有

系理 设 $f(x)$ 是 q 元周期序列 $\mathbf{a}$ 的极小多项式，那么 $\mathbf{a}$ 有有理分式表示 $\frac{g(x)}{f(x)}$, 其中 $(f(x), g(x))=1$, 而且 $f(x)$ 是产生 $\mathbf{a}$ 的任一线性移位寄存器的联接多项式的因式.

定理 5 设 $f(x)$ 是 q 元周期序列 $\mathbf{a}$ 的极小多项式. 那么 $f(x)$ 的周期 $p(f)$ 等于 $\mathbf{a}$ 的周期 $p(\mathbf{a})$.

证. 设

$$\sum_{i=0}^{\infty} a_i x^i=\frac{g(x)}{f(x)}, \tag{7}$$

再设 $p(f)=l$, 那么 $f(x)\mid x^l-1$, 即有 $d(x)\in \mathbf{F}_q[x]$ 使

$$1-x^l=f(x)d(x).$$

于是

$$\sum_{i=0}^{\infty} a_i x^i=\frac{g(x)}{f(x)}=\frac{g(x)d(x)}{f(x)d(x)}=\frac{g(x)d(x)}{1-x^l}.$$

由 $\partial^0 g(x)<\partial^0 f(x)$ 推出 $\partial^0 g(x)d(x)<\partial^0(1-x^l)=l$. 记

$$h(x)=g(x)d(x)=h_0+h_1x+h_2x^2+\cdots+h_{l-1}x^{l-1},$$

那么

$$\sum_{i=0}^{\infty} a_i x^i=\frac{h(x)}{1-x^l}=h(x)(1+x^l+x^{2l}+\cdots)$$
$$=h(x)+h(x)x^l+h(x)x^{2l}+\cdots.$$

比较系数可得

$$a_{\lambda l+k}=h_k=a_k,\ k=0,\ 1,\ 2,\ \cdots,\ l-1;\ \lambda=0,\ 1,\ 2,\ \cdots.$$

因此 $p(\mathbf{a})\mid l$.

再设 $p(\mathbf{a})=l'$. 那么

$$\sum_{i=0}^{\infty} a_i x^i=\frac{h_1(x)}{1-x^{l'}}, \tag{10}$$

其中 $h_1(x)\in \mathbf{F}_q[x]$, $\partial^0 h_1(x)<l'$. 那么由(7), (10)两式推出

$$f(x)h(x)=(1-x^{l'})g(x).$$

因 $f(x)$ 是 $\mathbf{a}$ 的极小多项式, $(f(x),\ g(x))=1$, 因此 $f(x)\mid 1-x^{l'}$, 于是 $p(f)\mid l'$.

因此 $p(f)=p(\mathbf{a})$.

系理 1 设 $f(x)$ 是 $\mathbf{F}_q$ 上的零次项等于 1 的不可约多项式, 那么 $G(f)$ 中的非零 q 元周期序列都以 $f(x)$ 为极小多项式, 而它们的周期都等于 $f(x)$ 的周期.

系理 2 设 q 元周期序列 $\mathbf{a}$ 有一个有理分式表示 $\dfrac{g(x)}{f(x)}$, 那么 $p(\mathbf{a})\mid p(f)$.

证. 设 $\mathbf{a}$ 的极小多项式是 $f_1(x)$, 那么根据定理 4, $f_1(x)\mid f(x)$. 因此 $p(f_1)\mid p(f)$. 根据定理 5 又有 $p(\mathbf{a})=p(f_1)$. 所以 $p(\mathbf{a})\mid p(f)$.

这样, 我们利用 q 元周期序列的有理分式表示法导出了本章 §2 的全部主要结论. 我们再指出怎样利用 q 元周期序列的有理分式表示法来讨论 $G(f)$ 中的平移等价类(这里 f 是 $\mathbf{F}_q$ 上的一个零次项等于 1 的多项式), 即得出 §3 中的主要结论定理 2, 3, 4. 首先, 显而易见, 根据定理 3 的系理, §3 定理 2 是下面这个关于部分分式的引理的直接推论.

引理 1 设 $f(x)$, $f_1(x)$, $f_2(x)$, $g(x)\in \mathbf{F}_q[x]$, $f(x)=f_1(x)f_2(x)$, $(f_1(x),\ f_2(x))=1$ 而 $\partial^0 g(x)<\partial^0 f(x)$, $\partial^0 f_1(x)>0$, $\partial^0 f_2(x)>0$. 那么有 $g_1(x)$, $g_2(x)\in \mathbf{F}_q[x]$, $\partial^0 g_1(x)<\partial^0 f_1(x)$, $\partial^0 g_2(x)<\partial^0 f_2(x)$ 使

$$\frac{g(x)}{f(x)}=\frac{g_1(x)}{f_1(x)}+\frac{g_2(x)}{f_2(x)},\tag{11}$$

而且适合上述条件的 $g_1(x)$, $g_2(x)$ 是唯一确定的.

证. 由假设 $(f_1(x),f_2(x))=1$, 根据第一章§2定理2的系理, 有 $h_1(x),h_2(x)\in\mathbf{F}_q[x]$ 具有性质

$$1=h_1(x)f_1(x)+h_2(x)f_2(x).$$

用 $g(x)$ 乘上式, 得

$$g(x)=g(x)h_1(x)f_1(x)+g(x)h_2(x)f_2(x).\tag{12}$$

用 $f_2(x)$ 去除 $g(x)h_1(x)$, 得

$$g(x)h_1(x)=q(x)f_2(x)+g_2(x),\quad \partial^0 g_2(x)<\partial^0 f_2(x).$$

将上式代入(12)式右方, 得

$$g(x)=g_2(x)f_1(x)+(g(x)h_2(x)+f_1(x)q(x))f_2(x).$$

令 $g_1(x)=g(x)h_2(x)+f_1(x)q(x)$, 则有

$$g(x)=g_2(x)f_1(x)+g_1(x)f_2(x).\tag{13}$$

因上式左方及右方第一项的次数都 $<\partial^0 f(x)$, 故 $\partial^0(g_1(x)\cdot f_2(x))<\partial^0 f(x)$. 但 $\partial^0 f(x)=\partial^0(f_1(x)f_2(x))=\partial^0 f_1(x)+\partial^0 f_2(x)$ 而 $\partial^0(g_1(x)f_2(x))=\partial^0 g_1(x)+\partial^0 f_2(x)$, 故 $\partial^0 g_1(x)<\partial^0 f_1(x)$. 用 $f(x)$ 去除(13)式两边就得出(11)式.

再证 $g_1(x)$, $g_2(x)$ 的唯一性, 设又有 $k_1(x)$, $k_2(x)\in\mathbf{F}_q[x]$, $\partial^0 k_1(x)<\partial^0 f_1(x)$, $\partial^0 k_2(x)<\partial^0 f_2(x)$ 使下式成立:

$$\frac{g(x)}{f(x)}=\frac{k_1(x)}{f_1(x)}+\frac{k_2(x)}{f_2(x)}.$$

将上式双方乘以 $f(x)=f_1(x)f_2(x)$, 得

$$g(x)=k_2(x)f_1(x)+k_1(x)f_2(x)\tag{14}$$

从(13)式减去(14)式, 得

$$(g_2(x)-k_2(x))f_1(x)=-(g_1(x)-k_1(x))f_2(x).$$

因 $(f_1(x),f_2(x))=1$, 故 $f_2(x)\mid(g_2(x)-k_2(x))$. 但 $\partial^0(g_2(x)-k_2(x))<\partial^0 f_2(x)$, 故 $g_2(x)-k_2(x)=0$, 因此 $g_2(x)=k_2(x)$, 随之也有 $g_1(x)=k_1(x)$.

其次，在§3中曾经指出该节定理3是该节定理2和引理4的推论. 现在我们利用q元周期序列的有理分式表示法再给出该节引理4另一个证明.

设$f_i(x)(i=1, 2, \cdots, r)$是$\mathbf{F}_q$上$r$个两两互素的零次项等于1的$n_i$次多项式，$n_i\geqslant 1$. 再设$\mathbf{a}_i\in G(f_i), i=1,2,\cdots,r$. 我们要证明

$$p(\mathbf{a}_1+\mathbf{a}_2+\cdots+\mathbf{a}_r)=[p(\mathbf{a}_1), p(\mathbf{a}_2), \cdots, p(\mathbf{a}_r)].$$

设 $\mathbf{a}_i=(a_{i0}, a_{i1}, a_{i2}, \cdots), i=1, 2, \cdots, r.$

再设$\mathbf{a}_i$的极小多项式是$m_i(x)$，那么$p(\mathbf{a}_i)=p(m_i)$，$m_i(x)|f_i(x)$而

$$\sum_{j=0}^{\infty} a_{ij}x^j=\frac{g_i(x)}{m_i(x)}, \ i=1, 2, \cdots, r.$$

那么$\mathbf{a}_1+\mathbf{a}_2+\cdots+\mathbf{a}_r$有有理分式表示

$$\sum_{j=0}^{\infty}\left(\sum_{i=1}^{r} a_{ij}\right)x^j=\sum_{i=1}^{r}\left(\sum_{j=0}^{\infty} a_{ij}x^j\right)=\sum_{i=1}^{r}\frac{g_i(x)}{m_i(x)}$$

$$=\frac{\sum\limits_{i=1}^{r} m_1(x)m_2(x)\cdots m_{i-1}(x)g_i(x)m_{i+1}(x)\cdots m_r(x)}{m_1(x)m_2(x)\cdots m_r(x)}$$

因$f_1(x), f_2(x), \cdots, f_r(x)$两两互素，所以$m_1(x), m_2(x),\cdots, m_r(x)$两两互素，于是

$$\Big(m_1(x)m_2(x)\cdots m_r(x), \sum_{i=1}^{r}m_1(x)m_2(x)\cdots m_{i-1}(x)$$
$$\times g_i(x)m_{i+1}(x)\cdots m_r(x)\Big)=1.$$

因此$m_1(x)m_2(x)\cdots m_r(x)$是$\mathbf{a}_1+\mathbf{a}_2+\cdots+\mathbf{a}_r$的极小多项式. 于是

$$p(\mathbf{a}_1+\mathbf{a}_2+\cdots+\mathbf{a}_r)=p(m_1m_2\cdots m_r).$$

这样问题就化为证明下面这个引理.

引理2 设$m_1(x), m_2(x), \cdots, m_r(x)$是$\mathbf{F}_q[x]$中$r$个两两互素的零次项等于1的多项式，那么

$$p(m_1m_2\cdots m_r)=[p(m_1), p(m_2), \cdots, p(m_r)].$$

证. 设 $p(m_i)=l_i$，即 l_i 是最小正整数使 $m_i(x)|x^{l_i}-1$. 令 $l=[l_1, l_2, \cdots, l_r]$. 那么 $m_i(x)|x^l-1$. 因 $m_1(x), m_2(x), \cdots, m_r(x)$ 两两互素，根据唯一因式分解定理推出 $m_1(x)m_2(x)\cdots m_r(x)|x^l-1$. 因此 $p(m_1m_2\cdots m_r)|l$.

其次，设 $l'=p(m_1m_2\cdots m_r)$. 那么 $m_1m_2\cdots m_r|x^{l'}-1$，于是 $m_i|x^{l'}-1$，$i=1, 2, \cdots, r$. 因此 $p(m_i)=l_i|l'$. 于是 $l=[p(m_1), p(m_2), \cdots, p(m_r)]|l'$.

由 $l'|l$ 及 $l|l'$ 推出 $l=l'$.

同样显而易见，根据定理 3 的系理，§ 3 定理 4 是下面这另一个关于部分分式的引理的推论.

引理 3 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个零次项等于 1 的多项式，e 是一个正整数. 再设 $g(x)\in\mathbf{F}_q[x]$ 而 $\partial^0 g(x)<\partial^0 f(x)^e$. 那么有 $g_1(x), g_2(x), \cdots, g_e(x)\in\mathbf{F}_q[x]$，$\partial^0 g_i(x)<\partial^0 f(x)$，$i=1, 2, \cdots, e$，使

$$\frac{g(x)}{f(x)^e}=\frac{g_1(x)}{f(x)}+\frac{g_2(x)}{f(x)^2}+\cdots+\frac{g_e(x)}{f(x)^e}, \qquad (15)$$

而且适合上述条件的 $g_1(x), g_2(x), \cdots, g_r(x)$ 是唯一确定的.

证. 用 $f(x)^{e-1}$ 去除 $g(x)$，将所得的商记作 $g_1(x)$，余式记作 $r_1(x)$，则 $\partial^0 g_1(x)<\partial^0 f(x)$，$\partial^0 r_1(x)<\partial^0 f(x)^{e-1}$；再用 $f(x)^{e-2}$ 去除 $r_1(x)$，将所得的商记作 $g_2(x)$，余式记作 $r_2(x)$，则 $\partial^0 g_2(x)<\partial^0 f(x)$，$\partial^0 r_2(x)<\partial^0 f(x)^{e-2}$；如此下去：

$$g(x)=g_1(x)f(x)^{e-1}+r_1(x)$$
$$r_1(x)=g_2(x)f(x)^{e-2}+r_2(x)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_{e-2}(x)=g_{e-1}(x)f(x)+r_{e-1}(x).$$

令 $g_e(x)=r_{e-1}(x)$，那么 $g_1(x), g_2(x), \cdots, g_e(x)$ 的次数都小于 $f(x)$ 的次数. 由这些方程一起推出

$$g(x)=g_1(x)f(x)^{e-1}+g_2(x)f(x)^{e-2}+\cdots+g_{e-1}(x)f(x)+g_e(x)$$

用 $f(x)^e$ 去除上式双方就得到(15)式.

至于 $g_1(x), g_2(x), \cdots, g_e(x)$ 是唯一确定的这一点则是带余除法中商式和余式是唯一确定的推论.

这样我们就利用 q 元周期序列的有理分式表示法导出了本章§3的所有重要结论. 我们建议读者再利用这一方法去讨论本章§10中的几个例子.

最后,我们来介绍 q 元周期序列的根表示法.我们先证明

引理 4 设 $f(x)\in \mathbf{F}_q[x]$, 则有正整数 N 存在使 $\mathbf{F}_{q^N}$ 包有 $f(x)$ 的全部根.

证. 将 $f(x)$ 在 $\mathbf{F}_q[x]$ 中分解成不可约因式的乘积

$$f(x)=f_1(x)^{e_1}f_2(x)^{e_2}\cdots f_r(x)^{e_r},$$

其中 $f_1(x), f_2(x), \cdots, f_r(x)$ 是 $\mathbf{F}_q[x]$ 中两两不同的不可约多项式. 设 $\partial^0 f_i(x)=n_i, i=1, 2, \cdots, r$. 那么根据第一章§4引理2, $f_i(x)\,|\,x^{q^{n_i}}-x, i=1, 2, \cdots, r$. 令 $N=[n_1, n_2, \cdots, n_r]$. 那么 $x^{q^{n_i}}-x\,|\,x^{q^N}-x$. 因此 $f_i(x)\,|\,x^{q^N}-x$. 因 $\mathbf{F}_{q^N}$ 的全部元素即是 $x^{q^N}-x$ 的全部根,所以 $f_i(x)$ 的全部根都在 $\mathbf{F}_{q^N}$ 之中. 于是 $f(x)$ 的全部根都在 $\mathbf{F}_{q^N}$ 之中.

设 $f(x)\in \mathbf{F}_q[x], \partial^0 f(x)=n$. 根据引理4可设 $f(x)$ 的根,都在某一个有限域 $\mathbf{F}_{q^N}$ 之中. 那么在 $\mathbf{F}_{q^N}$ 上, $f(x)$ 有分解式

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\ \alpha_i\in \mathbf{F}_{q^N}.$$

如果 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 两两相异,我们就说 $f(x)$ 无重根. 我们知道,当 $f(x)$ 在 $\mathbf{F}_q$ 上不可约时, $f(x)$ 无重根;如果 α 是它的一个根,那么 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ 就是 $f(x)$ 的全部根.

引理 5 设 $f(x), g(x)\in \mathbf{F}_q[x], \partial^0 g(x)<\partial^0 f(x)=n$, 而 $f(x)$ 的零次项等于1且无重根. 假定在 $\mathbf{F}_{q^N}$ 中 $f(x)$ 有分解式

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \alpha_i\in \mathbf{F}_{q^N}.$$

那么我们有

1) $\dfrac{g(x)}{f(x)}=\dfrac{\beta_1}{x-\alpha_1}+\dfrac{\beta_2}{x-\alpha_2}+\cdots+\dfrac{\beta_n}{x-\alpha_n}$,

其中 $\beta_1, \beta_2, \cdots, \beta_n\in\mathbf{F}_{q^N}$ 且由 $f(x)$ 和 $g(x)$ 唯一确定.

2) $(f(x), g(x))=1$ 当且仅当 $\beta_1, \beta_2, \cdots, \beta_n$ 全不等于 0.

证. 1) 是引理 1 的特例.

现在去证明 2). 若 $\beta_1, \beta_2, \cdots, \beta_n$ 中有等于 0 的, 不妨设 $\beta_1, \beta_2, \cdots, \beta_r\neq 0$ 而 $\beta_{r+1}=\beta_{r+2}=\cdots=\beta_n=0$, $r<n$. 那么

$$\frac{g(x)}{f(x)}=\sum_{i=1}^{n}\frac{\beta_i}{x-\alpha_i}=\sum_{i=1}^{r}\frac{\beta_i}{x-\alpha_i}$$
$$=\frac{h(x)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)},$$

其中
$$h(x)=\sum_{i=1}^{r}\beta_i(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{i-1})\times(x-\alpha_{i+1})\cdots(x-\alpha_r),$$

另一方面,
$$\frac{g(x)}{f(x)}=\frac{g(x)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)}$$

因此
$$\frac{g(x)}{(x-\alpha_{r+1})\cdots(x-\alpha_n)}=h(x)$$

于是
$$(x-\alpha_{r+1})\cdots(x-\alpha_n)\mid g(x).$$

由此推出
$$(x-\alpha_{r+1})\cdots(x-\alpha_n)\mid (f(x), g(x)).$$

因此
$$(f(x), g(x))\neq 1.$$

反之,设 $(f(x), g(x))\neq 1$. 令 $d(x)=(f(x), g(x))$, 那么 $\partial^0 d(x)\geqslant 1$. 可以写

$$f(x)=f_1(x)d(x),\ g(x)=g_1(x)d(x).$$

设 $\partial^0 f_1(x)=r$, 那么 $r<n$. 再设 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 是 $f_1(x)$ 的全部根. 因 $f(x)$ 无重根, 所以 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 两两相异. 根据引理 1, 有

$$\frac{g(x)}{f(x)}=\frac{g_1(x)}{f_1(x)}=\frac{\beta_1'}{x-\alpha_1}+\cdots+\frac{\beta_r'}{x-\alpha_r},$$

其中 $\beta_1', \cdots, \beta_r' \in \mathbf{F}_{q^N}$. 由 $\beta_1, \beta_2, \cdots, \beta_n$ 的唯一性推出

$$\beta_1=\beta_1',\ \beta_2=\beta_2',\ \cdots,\ \beta_r=\beta_r',\ \beta_{r+1}=\cdots=\beta_n=0.$$

于是 $\beta_1, \beta_2, \cdots, \beta_n$ 中有等于 0 的.

这样引理 5 就完全证明了.

定理 6 设 $f(x)$ 是 $\mathbf{F}_q$ 上的零次项等于 1 的 n 次多项式, 并假定 $f(x)$ 无重根. 设 $f(x)$ 的 n 个根是 $\alpha_1, \alpha_2, \cdots, \alpha_n$, 它们属于某个 $\mathbf{F}_{q^N}$, 那么 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 都不等于0. 再设 $\mathbf{a}=(a_0, a_1, a_2, \cdots)$ 是一个 q 元周期序列.

1) 如果 $\mathbf{a}$ 以 $f(x)$ 为它的一个生成多项式, 那么存在着唯一的一组元素 $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbf{F}_{q^N}$ 使

$$a_k=\sum_{i=1}^{n}\lambda_i(\alpha_i^{-1})^k,\ k=0,\ 1,\ 2,\ \cdots \tag{16}$$

反过来, 如果有 $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbf{F}_{q^N}$ 使(16)式成立, 那么 $\mathbf{a}$ 以 $f(x)$ 为一个生成多项式.

2) 如果用 $f_i(x)$ 表 α_i 的极小多项式, 用 $f^*(x)$ 表 $\mathbf{a}$ 的极小多项式. 那么 $f_i(x) \mid f^*(x)$, 当且仅当 $\lambda_i \neq 0 (i=1, 2, \cdots, n)$. 因此, $\mathbf{a}$ 以 $f(x)$ 为极小多项式, 当且仅当 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 都不等于 0.

3) 如果 $f(x)$ 不可约, 设 α 是 $f(x)$ 的一个根, 那么 $f(x)$ 的全部根是 $\alpha_1=\alpha, \alpha_2=\alpha^q, \alpha_3=\alpha^{q^2}, \cdots, \alpha_n=\alpha^{q^{n-1}}$. 按(16)式来定义 $a_k, k=0, 1, 2, \cdots$. 那么 $\mathbf{a}=(a_0, a_1, a_2, \cdots)$ 是 q 元周期序列, 当且仅当 $\lambda_i^q=\lambda_{i+1}, i=1, 2, \cdots, n$ (我们约定 $\lambda_{n+1}=\lambda_1$).

证. 1) 设 $f(x)$ 是 $\mathbf{a}$ 的一个生成多项式, 那么 $\mathbf{a}$ 的形式幂级数表示可表成以 $f(x)$ 为分母的有理分式

$$\sum_{k=0}^{\infty}a_kx^k=\frac{g(x)}{f(x)},\ \partial^0 g(x)<\partial^0 f(x).$$

根据引理 5,

$$\sum_{k=0}^{\infty} a_k x^k = \frac{g(x)}{f(x)} = \sum_{i=1}^{n} \frac{\beta_i}{x-\alpha_i} = \sum_{i=1}^{n} \frac{-\beta_i \alpha_i^{-1}}{1-x\alpha_i^{-1}}$$

$$= \sum_{i=1}^{n} (-\beta_i \alpha_i^{-1}) \sum_{k=0}^{\infty} (x\alpha_i^{-1})^k$$

$$= \sum_{k=0}^{\infty} \left(\sum_{i=1}^{n} (-\beta_i \alpha_i^{-1})(\alpha_i^{-1})^k \right) x^k.$$

比较系数并令 $\lambda_i = -\beta_i \alpha_i^{-1}$ 即得(16)式. 由 $\beta_1, \beta_2, \cdots, \beta_n$ 的唯一性就推出 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 的唯一性.

反之,如有 $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbf{F}_{q^n}$ 使(16)式成立,那么

$$\sum_{k=0}^{\infty} a_k x^k = \sum_{k=0}^{\infty} \left(\sum_{i=1}^{n} \lambda_i (\alpha_i^{-1})^k \right) x^k = \sum_{i=1}^{n} \lambda_i (x\alpha_i^{-1})^k$$

$$= \sum_{i=1}^{n} \frac{\lambda_i}{1-x\alpha_i^{-1}} = \sum_{i=1}^{n} \frac{-\lambda_i \alpha_i}{x-\alpha_i} = \frac{g(x)}{f(x)}.$$

其中
$$g(x) = \sum_{i=1}^{n} -\lambda_i \alpha_i (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{i-1}) \times (x-\alpha_{i+1})\cdots(x-\alpha_n).$$

因 $a_k \in \mathbf{F}_q$ 对 $k=0, 1, 2, \cdots, f(x) \in \mathbf{F}_q[x]$, 所以 $g(x) \in \mathbf{F}_q[x]$. 因此 $\dfrac{g(x)}{f(x)}$ 是 $\mathbf{a}$ 的一个有理分式表示, $f(x)$ 是 $\mathbf{a}$ 的一个生成多项式.

2) 设 $f^*(x)$ 是 $\mathbf{a}$ 的极小多项式,那么有

$$\sum_{k=0}^{\infty} a_k x^k = \frac{g(x)}{f(x)} = \frac{g^*(x)}{f^*(x)}, \ (f^*(x), g^*(x)) = 1. \tag{17}$$

设
$$f^*(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r),$$
那么
$$f(x) = f^*(x)(x-\alpha_{r-1})(x-\alpha_{r-2})\cdots(x-\alpha_n).$$
因 $f^*(\alpha_i) = 0$ 对 $i=1, 2, \cdots, r$, 所以 $f_i(x) \mid f^*(x)$ 对 $i=1, 2, \cdots, r$. 又因 $f^*(\alpha_j) \neq 0$ 对 $j=r+1, \cdots, n$, 所以 $f_j(x) \nmid f^*(x)$ 对 $j=r+1, \cdots, n$. 根据引理 5,

$$\frac{g(x)}{f(x)} = \frac{\beta_1}{x-\alpha_1} + \frac{\beta_2}{x-\alpha_2} + \cdots + \frac{\beta_n}{x-\alpha_n},$$

$$\frac{g^*(x)}{f^*(x)}=\frac{\beta_1'}{x-\alpha_1}+\frac{\beta_2'}{x-\alpha_2}+\cdots+\frac{\beta_r'}{x-\alpha_r}.$$

因(17)式成立，由 β_i 的唯一性推出

$$\beta_1=\beta_1',\ \beta_2=\beta_2',\ \cdots,\ \beta_r=\beta_r',\ \beta_{r+1}=\beta_{r+2}=\cdots=\beta_n=0.$$

更因 $f^*(x)$ 是 $\mathbf{a}$ 的极小多项式，所以 $\beta_1, \beta_2, \cdots, \beta_r$ 都不等于 0. 但 $\lambda_i=-\beta_i\alpha_i^{-1}$，故 $\lambda_1, \lambda_2, \cdots, \lambda_r$ 都不等于 0 而 $\lambda_{r+1}=\lambda_{r+2}=\cdots=\lambda_n=0$. 因此 $f_i(x)\,|\,f^*(x)$，当且仅当 $\lambda_i\neq 0$.

3) 设 $f(x)$ 不可约，而

$$\alpha_1=\alpha,\ \alpha_2=\alpha^q,\ \alpha_3=\alpha^{q^2},\ \cdots,\ \alpha_n=\alpha^{q^n}$$

是它的全部 n 个根．那么 $\alpha_i^q=\alpha_{i+1}$, $i=1, 2, \cdots, n$ (我们约定 $\alpha_{n+1}=\alpha_1$)．我们知道，$\mathbf{a}$ 是 q 元序列，当且仅当 $a_k^q=a_k$, $k=0, 1, 2, \cdots$. 我们有

$$a_k^q=\left[\sum_{i=1}^n\lambda_i(\alpha_i^{-1})^k\right]^q=\sum_{i=1}^n\lambda_i^q(\alpha_{i+1}^{-1})^k,\ k=0, 1, 2, \cdots.$$

那么由 λ_i 的唯一性可推知，$a_k^q=a_k$, $k=0, 1, 2, \cdots$, 当且仅当 $\lambda_i^2=\lambda_{i+1}$, $i=1, 2, \cdots, n$.

这样定理 6 就完全证明了．

如果 $f(x)$ 是 $\mathbf{F}_q$ 上的一个零次项等于 1 的无重根的 n 次多项式，$\alpha_1, \alpha_2, \cdots, \alpha_n$ 是它的 n 个根，而 $\mathbf{a}$ 是一个 q 元周期序列，它以 $f(x)$ 为它的一个生成多项式，我们把 (16) 式叫做 $\mathbf{a}$ 的根表示法．特别，如果 $f(x)$ 不可约，那么 $\alpha_1, \alpha_2, \cdots, \alpha_n\in\mathbf{F}_{q^n}$. 对 $\alpha\in\mathbf{F}_{q^n}$, 定义

$$\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}(\alpha)=\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}}$$

那么根据定理 6 中的 3)，可将(16)式写作

$$a_k=\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}[\lambda_1(\alpha_1^{-1})^k],\ k=0, 1, 2, \cdots.$$

我们把它叫做 q 元周期序列 $\mathbf{a}$ 的迹表示法．(当 $f(x)$ 是本原多项式，它在本章 § 4 中已经出现过．)也可以仿照 § 4，利用根表示法来讨论 q 元周期序列的采样，我们就不重复了．

第四章 纠错码导引

纠错码的内容非常丰富，是编码理论的重要组成部分，分为分组码和树码（主要是卷积码）两大类. 本章是导引性质的一章，包括的内容很少. 在这一章里我们先介绍分组码的一些基本概念，并以 Hamming 码为例来阐明这些概念. 随后我们介绍了 BCH 码和它的译码，这是很重要的一类纠正多个差错的分组码. 最后我们介绍了 Reed-Solomon 码，这是一类很好的纠正成区间差错的分组码. 至于卷积码，我们并没有进行任何讨论. 对纠错码有兴趣的读者，在读完本章后，可阅读本书所附参考书目中的[17]，[18]，[26]，[27]，[28]等.

§1 数字通信与纠错码

通信是将甲地的信息传送到乙地. 通常把甲地叫做信息源，也叫发方，把乙地叫做收信者，也叫收方. 最简化的通信模型可用下面的框图来表示：

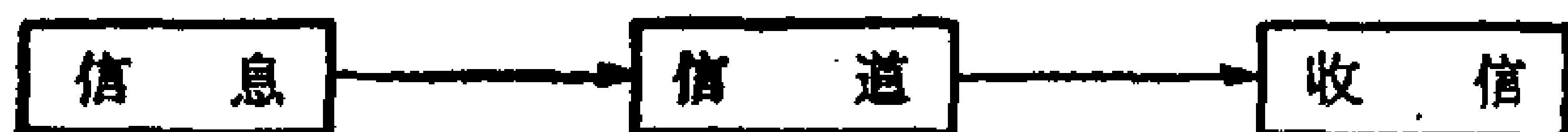


图 1

信道包括信息的调制（如将信息源的信息调制成电讯号），发送，传信介质（如空气或电线等），接收和解调（即将接收到的电讯号还原成信息源发送的信息）等部分. 传送的信息可以是声音，可以是文字和图象，也可以是数字. 例如电话和广播传送的是声音，电视和无线电传真传送的是文字和图象，而电

报传送的则是数字信息．将信息源的信息转化成数字信息传送给收信者就叫数字通信．工程上最易实现的是二元数字信息的传送．所谓二元数字信息就是用有限长的二元元素组

$$(a_0, a_1, a_2, \cdots, a_{k-1}), \quad a_i=0 \text{ 或 } 1$$

代表的信息．可以把 0 和 1 看作二元有限域 $\mathbf{F}_2$ 中的元素．通常是用同样长的二元元素组来代表一个信息集合中的信息．例如可以用 32 个二元 5 元素组(即长为 5 的二元元素组)来代表诸英文字母和有关标点符号，如图 2 所示．也可以说是用 $\mathbf{F}_2$ 上 5 维行向量空间 $V_5(\mathbf{F}_2)$ 中的向量来代表诸英文字母和有关标点符号．这样 $V_5(\mathbf{F}_2)$ 中的向量就是数字信息．

表 1

元素组	英文字母或标点符号
0 0 0 0 0	空格
0 0 0 0 1	*a*
0 0 0 1 0	*b*
0 0 0 1 1	*c*
0 0 1 0 0	*d*
0 0 1 0 1	*e*
0 0 1 1 0	*f*
0 0 1 1 1	*g*
⋮	⋮
1 1 0 1 0	*z*
1 1 0 1 1	,
1 1 1 0 0	.
1 1 1 0 1	?
1 1 1 1 0	!
1 1 1 1 1	—

数字信息在传送过程中可能受到种种干扰(如对于无线电信号来说，自然界存在的电磁源以及其他无线电系统发射的信号等等)，这样接收到的数字信息可能就不是原来信息源发送的数字信息．为了使信息源发送的数字信息能正确地传送到收信者，可以采取种种技术上的措施．更好的办法则是在采用种种技术上的措施的同时，再采用抗干扰编码的办法．这就是说，在数字

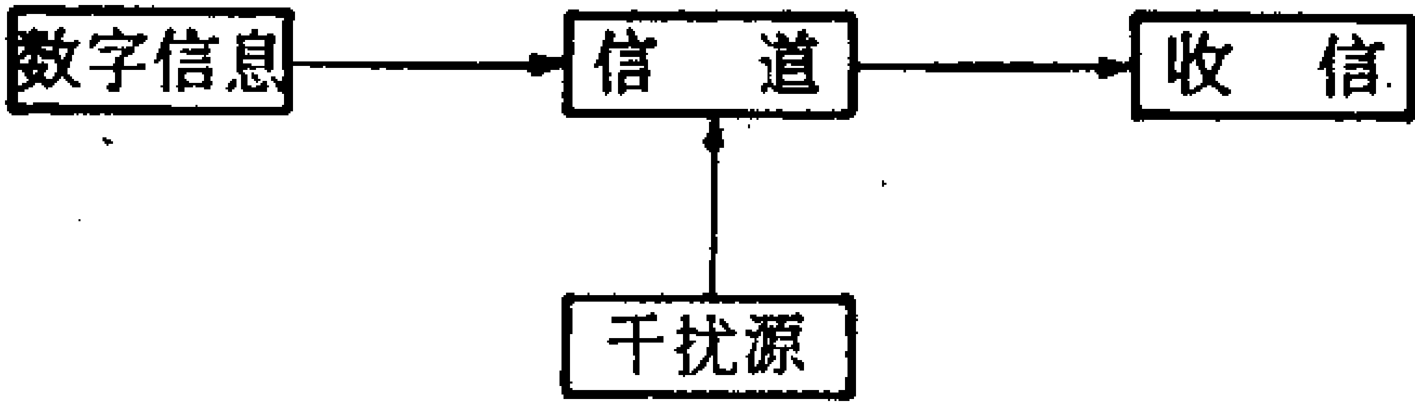


图 2

信息传送之前先进行一次抗干扰编码，然后再发送抗干扰编码后的数字信息．抗干扰编码有检错编码和纠错编码．

举上面的例子来说，原来的数字信息的集合是 $V_5(\mathbf{F}_2)$．一个原始数字信息是一个5维行向量 $(c_0, c_1, c_2, c_3, c_4)$．我们把这个5维行向量扩充成一个6维行向量

$$\sigma: (c_0, c_1, c_2, c_3, c_4) \to \left(c_0, c_1, c_2, c_3, c_4, \sum_{i=0}^{4} c_i\right),$$

其中求和是在 $\mathbf{F}_2$ 中求和．信息源不发送 $(c_0, c_1, c_2, c_3, c_4)$，而发送

$$\sigma((c_0, c_1, c_2, c_3, c_4)) = \left(c_0, c_1, c_2, c_3, c_4, \sum_{i=0}^{4} c_i\right).$$

记 $$\sigma(V_5(\mathbf{F}_2)) = \{\sigma(\mathbf{c}) \mid \mathbf{c} \in V_5(\mathbf{F}_2)\},$$

那么 $$\sigma(V_5(\mathbf{F}_2)) \subset V_6(\mathbf{F}_2).$$

我们把 $\sigma(V_5(\mathbf{F}_2))$ 叫做码，把其中的向量叫做*码字*，而把 $V_6(\mathbf{F}_2)$中的向量叫做字．注意 $\sigma(V_5(\mathbf{F}_2))$中的向量有一个特征性质，就是它的6个分量之和一定是0．换句话说，$V_6(\mathbf{F}_2)$中的字是一个码字，当且仅当它的6个分量之和是0．这样当发方发送一个码字

$$\mathbf{c} = (c_0, c_1, c_2, c_3, c_4, c_5), \sum_{i=0}^{5} c_i = 0$$

后，设收方收到的字是

$$\mathbf{r} = (r_0, r_1, r_2, r_3, r_4, r_5).$$

计算一下 $\mathbf{r}$ 的6个分量之和 $\sum_{i=0}^{5} r_i$．如果 $\sum_{i=0}^{5} r_i \neq 0$，那就在传送过程中一定出现差错，确切地说，有奇数个位(即分量)发生差错(即0传成1或1传成0)．当然如果 $\sum_{i=0}^{5} r_i = 0$，那么在传送过程中可能不发生差错，也可能偶数个位发生差错．因此如果码字在信道中传送时顶多出现1个差错(即或者不出现差错，或者只1位出现差错)，那么收方肯定可以查出有没有

差错. $\sigma(V_5(\mathbf{F}_2))$这个码叫做奇偶校验码，它是检错码的一个最简单的例子. 数字通信中采用它，可以检查出 $\leqslant 1$ 个差错. 从 $V_5(\mathbf{F}_2)$ 映入 $V_6(\mathbf{F}_2)$ 的映射σ 就叫检错编码，它在工程上是不难实现的. 码 $\sigma(V_5(\mathbf{F}_2))$中码字的前5位叫做它的信息位，而最后一位是添上的校验位. 计算收到的字 $\mathbf{r}$ 的6个分量之和叫做检错措施，它在工程上也是不难实现的.

一般地，设信息源的原始数字信息的集合是 $V_k(\mathbf{F}_q)$，q 是一个素数的幂，而n是大于 k 的一个整数. 设σ是从 $V_k(\mathbf{F}_q)$ 映入 $V_n(\mathbf{F}_q)$ 的一个一一映射:

$$\sigma:\ V_k(\mathbf{F}_q)\to V_n(\mathbf{F}_q).$$

记

$$C=\sigma(V_k(\mathbf{F}_q)),$$

那么

$$C\subset V_n(\mathbf{F}_q).$$

设在数字通信中采用C作为码，那么C中的向量就叫码字，n叫做码长，而码字的分量叫做码元. 现在码元在 $\mathbf{F}_q$ 中取值，所以C就叫q元码. 我们还把 $V_n(\mathbf{F}_q)$ 中的向量叫做字，而字的n个分量从左到右依序叫做第0位置的分量，第1位置的分量，第2位置的分量，…，第$n-1$位置的分量，而码字的n个码元则从左到右依序叫做第0位置的码元，第1位置的码元，第2位置的码元，…，第$n-1$位置的码元. 发方发送一个码字后，如果在传送过程中码字有 $\leqslant t$ 个位置的码元（或分量）发生差错，收方从收到的字就可以判断在传送过程中有没有差错发生，那么C就叫码长n的可检查出t个差错的检错码，而σ就叫检错编码.

在双向信道的情形，即收方也可以发送信息给发方，当收方从收到的字查出码字在传送过程中有差错发生时，就可以通知发方重发一次这个码字. 但在单向信道的情形，却不能这样做. 确实有单向信道的情形存在. 例如，信息源有一组原始数字信息，将它们输送进一个存储系统（如电子计算机的

磁带）．这时可将这个存储系统看作信道．输进去之后，原始数字信息即不再保存．过了一段时间之后，需要取用存储系统中所存储的数字信息，可以把取用者看作收信者．如果存储原始数字信息时，将原始数字信息进行检错编码以后再存入存储系统，即使取用者查出所存某一数字信息有错，他也没有办法通知信息源再重发一次这一数字信息．又如为了减轻人造星体的重量，有时人造星体只载发送设备而不载接收设备．这时人造星体只能发送电信号给地球上的接收站，而不能接收地球上接收站发出的电信号．在单向信道的情形，采用检错码尽管可以检查出码字在传送过程中是否出现差错，但当检查出差错后却无助于收信者获得信息源发送的码字．这时就要采用**纠错码**．

仍设原始数字信息集合是 $V_k(\mathbf{F}_q)$，而 $n>k$，σ 是从 $V_k(\mathbf{F}_q)$ 映入 $V_n(\mathbf{F}_q)$ 的一个一一映射：

$$\sigma:\ V_k(\mathbf{F}_q)\to V_n(\mathbf{F}_q).$$

仍记 $C=\sigma(V_k(\mathbf{F}_q))$．设在数字通信中采用 C 作为码．发方发送一个码字后，如果在传送过程中码字有 $\leqslant t$ 个位置的码元（或分量）发生差错，而收方从收到的字可以正确译出发方发送的码字，那么这个码就叫码长 n 的**可纠正 t 个差错的纠错码**，σ 就叫**纠错编码**．

采用抗干扰编码的数字通信有以下的框图：

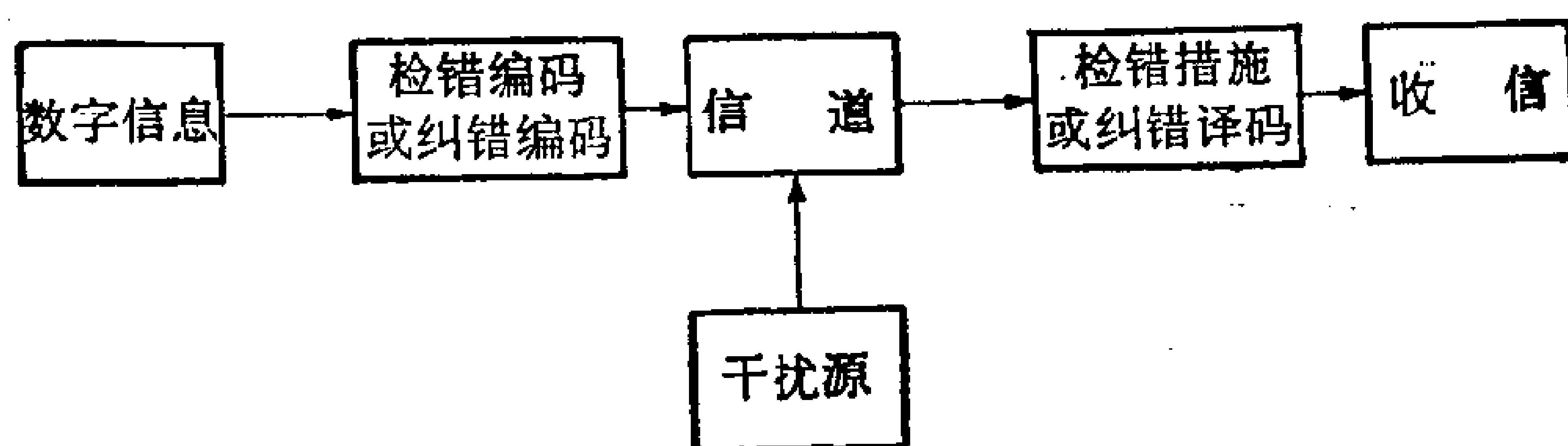


图　3

检错编码或纠错编码由编码器来实现，而检错措施或纠错译

码由检错设备或译码器来实现.

通常我们把 $\frac{k}{n}\log_2 q$ 叫做码 $C=\sigma(V_k(\mathbf{F}_q))$ 的信息率. 在数字通信中,我们要针对具体的需要,选择信息率高,检错(或纠错)能力大,而编码和译码都比较简单的码.

我们再举一个纠错码的例子. 设信息源的原始数字信息是 $V_4(\mathbf{F}_2)$ 中的 4 个向量

$$(0\,0)\quad(0\,1)\quad(1\,0)\quad(1\,1).$$

对它们进行纠错编码:

$$\sigma((0\,0))=(1\,0\,0\,1\,0)$$
$$\sigma((0\,1))=(0\,1\,0\,0\,1)$$
$$\sigma((1\,0))=(1\,0\,1\,0\,1)$$
$$\sigma((1\,1))=(0\,1\,1\,1\,0).$$

令

$$C=\sigma(V_2(\mathbf{F}_2)),$$

那么 $C=\{(1\,0\,0\,1\,0),\ (0\,1\,0\,0\,1),\ (1\,0\,1\,0\,1),\ (0\,1\,1\,1\,0)\}$ 就是一个码长 5 的、信息率 2/5 的码. 假定发方发送了 C 的一个码字,收方收到一个字 $\mathbf{r}\in V_5(\mathbf{F}_2)$,问题是将 $\mathbf{r}$ 译成哪一个码字. 通常译码采取所谓"极大似然译码方法",这就是说,看 $\mathbf{r}$ 最"象"哪个码字就把它译成哪个码字. 至于什么是"象",这最好在 $V_5(\mathbf{F}_2)$ 中引进 Hamming 距离来加以说明.

设 $\mathbf{a}$, $\mathbf{b}$ 是 $V_n(\mathbf{F}_q)$ 中的向量. 写

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1}),$$
$$\mathbf{b}=(b_0,\ b_1,\ b_2,\ \cdots,\ b_{n-1}).$$

定义 $\rho(\mathbf{a},\ \mathbf{b})$ 为 $\mathbf{a}$ 和 $\mathbf{b}$ 的相应位置分量不相等的个数,即 $a_i\neq b_i$ 的 i 的个数:

$$\rho(\mathbf{a},\ \mathbf{b})=\sum_{a_i\neq b_i}1$$

我们把 $\rho(\mathbf{a},\ \mathbf{b})$ 叫做 $\mathbf{a}$ 和 $\mathbf{b}$ 之间的 Hamming 距离,简称距离.

例如，对于 C 中的码字来说

$$\rho((10010),(01001))=4,$$
$$\rho((10010),(10101))=3,$$
$$\rho((10010),(01110))=3,$$
$$\rho((01001),(10101))=3,$$
$$\rho((01001),(01110))=3,$$
$$\rho((10101),(01110))=4.$$

现在设收方收到的字是 $\mathbf{r}\in V_5(\mathbf{F}_2)$，那么 $\mathbf{r}$ 和那个码字的距离最小，我们就说 $\mathbf{r}$ 和这个码字最"象"．这时我们就把 $\mathbf{r}$ 译成这个码字．因此极大似然译码方法是基于"收到的字是从一个码字经错传尽可能少的位而来的可能性较从一个码字经错传较多位而来的可能性要大"这一前提的译码方法．从直观上来看，要求信道对每一位来说，正确传送的可能性比错误传送的可能性要大，是合乎情理的．否则这个信道就太不可靠了．从信道满足这一要求出发，就自然可以得出上面说的前提．

我们再回到上面举的例子，看如何根据极大似然译码方法来译码．假定收方收到的字是(10110)．计算一下这个字与 C 中码字的距离，发现它与(10010)的距离是1，而与其他三个码字的距离都大于1，那么我们就把(10110)译成(10010)．又如收到的字是(01101)，它与(01001)的距离是1，而与其他三个码字的距离都大于1，那么我们就把(01101)译成(01001)．但是如果收到的字是(11011)；它与(10010)和(01001)的距离都是2，而与其余两个码字的距离都是3，这时根据极大似然译码方法就不能确定把(11011)译成(10010)或(01001)．

我们可以根据极大似然译码方法列出一个译码表．这个表的第一行是 C 中的4个码字．每个码字下面列出的字是应

表 2　译码表

码　字	10010	01001	10101	01110
其余的字	00010	11001	00101	11110
	11010	00001	11101	00110
	10110	01101	10001	01010
	10000	01011	10111	01100
	10011	01000	10100	01111
	11011	00000	00111	11100
	00011	11000	11111	00100

该译成这个码字的字．这种字一共 20 个，它们每一个都与唯一的一个码字的距离是 1 而与其余的码字的距离大于 1．虚线下的 8 个字是根据极大似然译码方法无法判断译成那个码字的字，它们每一个都与两个码字的距离是 2 而与其他两个码字的距离大于 2．这样，一个码字在传送过程中如果只错了一位，即只有一个码元传错，那么就可以从收到的字正确译出原来发送的码字；这只要到译码表中去找一下这个字在哪个码字的那一列就行了．但是如果一个码字在传送过程中错了两位以上，那么按译码表译码就会发生译码错误或无法译出．例如，设发方发出的码字 01001 错成 10001，按译码表就错译成 10101．又如，设发方发出的码字 10010 错成 00000，按译码表就无法译出，因 00000 在虚线下面．因此 C 是可纠一个差错的纠错码．

当然，当 n 大时，按译码表译码，查找的工作量很大．例如当码长 $n=100$ 时，二元码的译码表中一共有 2^{100} 个字．要从 2^{100} 个字的表里查出收到的一个字在哪一个码字的列里，即使用快速电子数字计算机也是难以完成的．因此在数字通信中，我们往往选用具有某种代数结构的纠错码，从而可利用这些码的代数特性来译码．

现在再回来讨论 $V_n(\mathbf{F}_q)$ 中的 Hamming 距离. 我们有

定理 1 $V_n(\mathbf{F}_q)$ 中的 Hamming 距离具有通常距离函数所具有的一些特性:

1)(自反性) 对任意 $\mathbf{a}\in V_n(\mathbf{F}_q)$,

$$\rho(\mathbf{a},\ \mathbf{a})=0.$$

2)(对称性) 对任意 $\mathbf{a},\ \mathbf{b}\in V_n(\mathbf{F}_q)$,

$$\rho(\mathbf{a},\ \mathbf{b})=\rho(\mathbf{b},\ \mathbf{a}).$$

3)(三角形不等式) 对任意 $\mathbf{a},\ \mathbf{b},\ \mathbf{c}\in V_n(\mathbf{F}_q)$,

$$\rho(\mathbf{a},\ \mathbf{b})+\rho(\mathbf{b},\ \mathbf{c})\geqslant\rho(\mathbf{a},\ \mathbf{c}).$$

证. 前两个性质是显然的. 至于第三个性质,设

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1}),$$

$$\mathbf{b}=(b_0,\ b_1,\ b_2,\ \cdots,\ b_{n-1}),$$

$$\mathbf{c}=(c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1}).$$

显然当 $a_i\neq c_i$ 时,一定有

$$a_i\neq b_i \quad 或 \quad b_i\neq c_i (i=0,\ 1,\ 2,\ \cdots,\ n-1).$$

因此

$$\rho(\mathbf{a},\ \mathbf{b})+\rho(\mathbf{b},\ \mathbf{c})\geqslant\rho(\mathbf{a},\ \mathbf{c}).$$

利用定理 1, 我们可以证明

定理 2 设 C 是码长 n 的一个码, 如果 C 中任意两个码字的距离都 $\geqslant t+1$, 那么 C 是可以检查出 t 个差错的检错码. 更进一步, 如果 C 中确有两个码字的距离等于 $t+1$, 那么 C 不能检查出 $t+1$ 个差错.

如果 C 中任意两个码字的距离都 $\geqslant 2t+1$, 那么 C 是可纠正 t 个差错的纠错码. 更进一步, 如果 C 中确有两个码字的距离等于 $2t+1$, 那么 C 不能纠正 $t+1$ 个差错.

证. 先设 C 中任意两个码字的距离都 $\geqslant t+1$. 假定信息源发送一个码字 $\mathbf{a}$, 并假定它在传送过程中错了 $\leqslant t$ 位, 即

有 $\leqslant t$ 个码元被传错，结果收到的字是 $\mathbf{r}$，即

$$\rho(\mathbf{a},\ \mathbf{r})\leqslant t.$$

因 C 中任意两个码字的距离都 $\geqslant t+1$，所以 $\mathbf{r}$ 如果不是 $\mathbf{a}$ 就肯定不是码字，因而就可以肯定传送过程中发生错误．因此 C 是可以检查出 t 个差错的检错码．

如果 C 中有两个码字 $\mathbf{a}$ 和 $\mathbf{b}$ 的距离等于 $t+1$，即

$$\rho(\mathbf{a},\ \mathbf{b})=t+1.$$

那么当发送的码字是 $\mathbf{a}$，传送过程中传错了 $t+1$ 个码元而错成 $\mathbf{b}$ 时，就无法从收到的 $\mathbf{b}$ 检查出错误．

再设 C 中任意两个码字的距离都 $\geqslant 2t+1$．假定信息源发送一个码字 $\mathbf{a}$，并假定它在传送过程中错了 $\leqslant t$ 位，结果收到的字是 $\mathbf{r}$，即

$$\rho(\mathbf{a},\ \mathbf{r})\leqslant t. \tag{1}$$

对任意 $\mathbf{b}\in C$，我们有

$$\rho(\mathbf{a},\ \mathbf{r})+\rho(\mathbf{r},\ \mathbf{b})\geqslant\rho(\mathbf{a},\ \mathbf{b})\geqslant 2t+1. \tag{2}$$

由(1)和(2)式就可以推出

$$\rho(\mathbf{r},\ \mathbf{b})\geqslant t+1.$$

这就是说 $\mathbf{r}$ 与任意一个不等于 $\mathbf{a}$ 的码字的距离都 $\geqslant t+1$，而与 $\mathbf{a}$ 的距离 $\leqslant t$．因此 $\mathbf{r}$ 与 $\mathbf{a}$ 的距离最小．这样根据极大似然译码方法就将 $\mathbf{r}$ 正确译成 $\mathbf{a}$．因此 C 是可以纠正 t 个差错的纠错码．

如果 C 中有两个码字 $\mathbf{a}$ 和 $\mathbf{b}$ 的距离是 $2t+1$，即

$$\rho(\mathbf{a},\ \mathbf{b})=2t+1,$$

那么总可以找到一个字 $\mathbf{r}$ 有性质

$$\rho(\mathbf{a},\ \mathbf{r})=t+1,\quad \rho(\mathbf{b},\ \mathbf{r})=t. \tag{3}$$

实际上，如果 $a_{i_1}\neq b_{i_1},\ a_{i_2}\neq b_{i_2},\ \cdots,\ a_{i_{2t+1}}\neq b_{i_{2t+1}}$，而

$$a_j=b_j,\ \text{对其余的}\ j,$$

那么令
$$r_{i_1}=a_{i_1},\ r_{i_2}=a_{i_2},\ \cdots,\ r_{i_t}=a_{i_t},$$
$$r_{i_{t+1}}=b_{i_{t+1}},\ r_{i_{t+2}}=b_{i_{t+2}},\ \cdots,\ r_{i_{2t+1}}=b_{i_{2t+1}},$$
$$r_j=a_j,\ \text{对其余的}\ j,$$
$\mathbf{r}=(r_0, r_1, r_2, \cdots, r_{n-1})$ 就符合条件(3). 这时当发送的码字是 $\mathbf{a}$, 传送过程中传错了 $t+1$ 个码元,错成 $\mathbf{r}$ 时,那么
$$\rho(\mathbf{r}, \mathbf{b})<\rho(\mathbf{r}, \mathbf{a}).$$
于是根据极大似然译码方法,就不能从收到的字 $\mathbf{r}$ 译出 $\mathbf{a}$. 这时就发生译码错误或无法译出.

这证明了定理 2.

从定理 2 可见,一个码 C 中两两码字的距离的极小值
$$\min\{\rho(\mathbf{a}, \mathbf{b})\,|\,\mathbf{a}, \mathbf{b}\in C, \mathbf{a}\neq\mathbf{b}\}$$
是衡量 C 的检错能力和纠错能力一个数. 我们把它叫做 C 的极小距离.

对任意 $\mathbf{a}=(a_0, a_1, a_2, \cdots, a_{n-1})\in V_n(\mathbf{F}_q)$, 我们定义 $w(\mathbf{a})$ 为 $\mathbf{a}$ 的不等于 0 的分量的个数,即
$$w(\mathbf{a})=\sum_{a_i\neq 0}1.$$
我们把 $w(\mathbf{a})$ 叫做 $\mathbf{a}$ 的 Hamming 重量, 简称 $\mathbf{a}$ 的重量, 并把码 C 中不等于 $\mathbf{0}$ 的码字的重量的极小值
$$\min\{w(\mathbf{a})\,|\,\mathbf{a}\in C, \mathbf{a}\neq 0\}$$
叫做 $\mathbf{a}$ 的极小重量.

我们再定义码的等价的概念. 设 C 和 C' 都是码长 n 的 q 元码. 再设有位置集合 $\{0, 1, 2, \cdots, n-1\}$ 的一个排列 $\{i_0, i_1, i_2, \cdots, i_{n-1}\}$, 即 $0\leqslant i_0, i_1, i_2, \cdots, i_{n-1}\leqslant n-1$ 而 $i_0, i_1, i_2, \cdots, i_{n-1}$ 两两不同. 如果以下条件成立: $(c_0, c_1, c_2, \cdots, c_{n-1})\in C$, 当且仅当$(c_{i_0}, c_{i_1}, c_{i_2}, \cdots, c_{i_{n-1}})\in C'$, 我们就说 C 和 C' 是等价的码. 显然等价的码有同样个数的码字. 两个等价的码并没有什么实质的区别.

§2 线 性 码

设 C 是个码长 n 的 q 元码，即 $C\subset V_n(\mathbf{F}_q)$. 我们知道，$V_n(\mathbf{F}_q)$ 是 $\mathbf{F}_q$ 上的 n 维向量空间. 如果 C 是 $V_n(\mathbf{F}_q)$ 的子空间，我们就说 C 是个 q 元*线性码*. 值得注意的是，当 $q=2$ 时，$V_n(\mathbf{F}_2)$ 的加法群的子群一定是子空间. 因此我们也可以说，如果 C 是 $V_n(\mathbf{F}_2)$ 的加法群的子群，C 就是二元线性码. 所以有时也把二元线性码叫做*群码*.

现在假定 C 是码长 n 的 q 元线性码，并假定 C 是 $V_n(\mathbf{F}_q)$ 的 k 维子空间，那么 C 一共含 q^k 个码字. 可以把 C 看作原始数字信息集合 $V_k(\mathbf{F}_q)$ 在某一编码 σ(即一一映射)之下的象

$$\sigma:\ V_k(\mathbf{F}_q)\to C.$$

设 $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{k-1}$ 是 C 的一组基. 令

$$G=\begin{pmatrix}\mathbf{v}_0\\ \mathbf{v}_1\\ \mathbf{v}_2\\ \vdots\\ \mathbf{v}_{k-1}\end{pmatrix},$$

那么 G 就是 $\mathbf{F}_q$ 上的一个秩为 k 的 $k\times n$ 矩阵. 如果记

$$\mathbf{v}_i=(v_{i0},\ v_{i1},\ v_{i2},\ \cdots,\ v_{in-1}),\quad 0\leqslant i\leqslant k-1,$$

那么

$$G=\begin{pmatrix}v_{00} & v_{01} & v_{02} & \cdots & v_{0n-1}\\ v_{10} & v_{11} & v_{12} & \cdots & v_{1n-1}\\ v_{20} & v_{21} & v_{22} & \cdots & v_{2n-1}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ v_{k-10} & v_{k-11} & v_{k-12} & \cdots & v_{k-1n-1}\end{pmatrix}.$$

因 $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \cdots\mathbf{v}_{k-1}$ 是 C 的一组基，所以 C 中任一码字 $\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{n-1})$ 都可以表成它们的线性组合而系数

属于 $\mathbf{F}_q$，而且表法是唯一的：

$$\mathbf{c}=a_0\mathbf{v}_0+a_1\mathbf{v}_1+a_2\mathbf{v}_2+\cdots+a_{k-1}\mathbf{v}_{k-1},\ a_i\in\mathbf{F}_q. \tag{1}$$

反过来，$\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{k-1}$ 的任意一个系数属于 $\mathbf{F}_q$ 的线性组合都是 C 中的码字．因此 G 叫做 C 的一个**生成矩阵**．利用矩阵乘法，也可以把(1)写成

$$\mathbf{c}=(a_0, a_1, a_2, \cdots, a_{k-1})G \tag{2}$$

我们可以把(1)或(2)看作是原始数字信息集合 $V_k(\mathbf{F}_q)$ 的一个编码（纠错编码或检错编码），即

$$\sigma((a_0, a_1, a_2, \cdots, a_{k-1}))=(a_0, a_1, a_2, \cdots, a_{k-1})G,$$
$$\text{对任意}(a_0, a_1, a_2, \cdots, a_{k-1})\in V_k(\mathbf{F}_q). \tag{3}$$

这个编码在工程上是可以实现的．当然当 q, n 和 k 大时，实现它需要相当多的设备．这个编码自然依赖于 G 的选择，即依赖于 C 的基的选择．如果 G_1 也是 C 的一个生成矩阵，即 G_1 的行向量也是 C 的一组基，那么

$$\sigma_1((a_0, a_1, a_2, \cdots, a_{k-1}))=(a_0, a_1, a_2, \cdots, a_{k-1})G_1,$$
$$\text{对任意}(a_0, a_1, a_2, \cdots, a_{k-1})\in V_k(\mathbf{F}_q),$$

就是原始数字信息集合 $V_k(\mathbf{F}_q)$ 的另一个编码．

根据第二章§3定理1我们知道，$\mathbf{F}_q$ 上的两个秩为 k 的 $k\times n$ 矩阵 G 和 G_1 是同一个码长 n 的、维数 k 的 q 元线性码 C 的两个生成矩阵，当且仅当有 $\mathbf{F}_q$ 上的 $k\times k$ 可逆矩阵 P 使 $PG=G_1$，再根据第二章§3定理3的系理2可知，当且仅当 G 和 G_1 行等价，即对其中之一的行进行初等变换可以将它化成另一个．因此要决定一切码长 n 的、维数 k 的 q 元线性码，只要定出 $\mathbf{F}_q$ 上的一组两两不行等价的秩为 k 的 $k\times n$ 矩阵即可，也即求出 $\mathbf{F}_q$ 上秩为 k 的 $k\times n$ 矩阵在行等价变换之下的标准形即可．这是一个纯代数问题，它在第二章§2定理5中已经解决．我们知道，可以对 G 的行进行初等变换，将 G 化为阶梯形矩阵

$$G_0=\begin{pmatrix} 0\cdots 0\ 1 & *\cdots * & 0 & *\cdots * & 0 & *\cdots *\cdots & 0 & *\cdots * \\ 0\cdots 0\ 0 & 0\cdots 0 & 1 & *\cdots * & 0 & *\cdots *\cdots & 0 & *\cdots * \\ 0\cdots 0\ 0 & 0\cdots 0 & 0 & 0\cdots 0 & 1 & *\cdots *\cdots & 0 & *\cdots * \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots & \cdots & \cdots\cdots & \cdots & \cdots\cdots \\ 0\cdots 0\ 0 & 0\cdots 0 & 0 & 0\cdots 0 & 0 & 0\cdots 0\cdots & 1 & *\cdots * \end{pmatrix},$$

第 i_0 列　　第 i_1 列　　第 i_2 列　　第 i_{k-1} 列

那么 G_0 也是 C 的一个生成矩阵. 把 G_0 的行自上而下地依序记作 $\mathbf{w}_0, \mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_{k-1}$. 那么 $\mathbf{w}_0, \mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_{k-1}$ 也是 C 的一组基. 当然也可以利用 G_0 来对原始数字信息集合 $V_k(\mathbf{F}_q)$ 进行编码

$$\sigma_0((a_0, a_1, a_2, \cdots, a_{k-1}))=(a_0, a_1, a_2, \cdots, a_{k-1})G_0,$$
$$\text{对任意}(a_0, a_1, a_2, \cdots, a_{k-1})\in V_k(\mathbf{F}_q). \tag{4}$$

令 $\sigma_0((a_0, a_1, a_2, \cdots, a_{k-1}))=(c_0, c_1, c_2, \cdots, c_{n-1})$,

那么注意到 G_0 的形状, 从(4)式容易看出

$$c_{i_0}=a_0,\ c_{i_1}=a_1,\ c_{i_2}=a_2,\ \cdots,\ c_{i_{k-1}}=a_{k-1};$$

而其余的 c_j 都是 $a_0, a_1, a_2, \cdots, a_{k-1}$ 的系数属于 $\mathbf{F}_q$ 的线性组合. 因此如按(4)将原始数字信息 $(a_0, a_1, a_2, \cdots, a_{k-1})$ 编码, 那么所得 C 中码字的第 i_0 位, 第 i_1 位, 第 i_2 位, …和第 i_{k-1} 位的码元分别和原始数字信息的第 0 位, 第 1 位, 第 2 位, …和第 $k-1$ 位的元素完全一样, 而其余各位则由它的第 i_0 位, 第 i_1 位, 第 i_2 位, …和第 i_{k-1} 位完全确定. 因此我们把 C 中码字的第 i_0 位, 第 i_1 位, 第 i_2 位, …和第 i_{k-1} 位看作它的信息位, 而把它的其余 $n-k$ 位看作是为了抗干扰而添上的校验位. 我们说 C 的信息位的个数是 k, 而它的校验位的个数是 $n-k$. 注意, C 的信息位的个数就等于它的维数. 当 C 是码长 n 而信息位个数等于 k 的 q 元线性码时, 我们也说 C 是个 q 元 (n, k) 线性码. 特别, 如果 G_0 是以下形状的矩阵

$$G_0=(I^{(k)},\ P^{(k,n-k)}),$$

其中 $I^{(k)}$ 是 $\mathbf{F}_q$ 上的 $k\times k$ 单位矩阵，而 $P^{(k,n-k)}$ 是 $\mathbf{F}_q$ 上任一 $k\times(n-k)$ 矩阵，那么这时 C 的前 k 位就可以看作它的信息位. 这时我们说 C 是*系统码*(或*组织码*). 显然任一线性码都等价于一个系统码.

仍设 C 是一个 q 元$(n,\ k)$线性码，而 G 是它的一个生成矩阵. 令

$$C^*=\{\mathbf{x}\,|\,\mathbf{x}\in V_n(\mathbf{F}_q)\text{而 }\mathbf{a}\mathbf{x}'=0,\ \text{对一切 }\mathbf{a}\in C\}.$$

那么根据第二章 §4 定理 2, C^* 是 $V_n(\mathbf{F}_q)$ 的一个 $n-k$ 维子空间. 因此 C^* 可以看作是一个 q 元$(n,\ n-k)$线性码. 我们把 C^* 叫做 C 的*对偶码*. 设 $\mathbf{u}_0,\ \mathbf{u}_1,\ \mathbf{u}_2,\ \cdots,\ \mathbf{u}_{n-k-1}$ 是 C^* 的一组基. 令

$$H=\begin{pmatrix}\mathbf{u}_0\\ \mathbf{u}_1\\ \mathbf{u}_2\\ \vdots\\ \mathbf{u}_{n-k-1}\end{pmatrix},$$

那么 H 就是 C^* 的一个生成矩阵，它是 $\mathbf{F}_q$ 上的一个秩为 $n-k$ 的 $(n-k)\times n$ 矩阵. 显然有，对任意 $\mathbf{x}\in V_n(\mathbf{F}_q)$:

$$\mathbf{x}\in C,\ \text{当且仅当 } H\mathbf{x}'=\mathbf{0}'.$$

因此 H 可用来判断 $V_n(\mathbf{F}_q)$ 中的一个字是否是 C 中的码字. H 又叫做 C 的一个*校验矩阵*. 设 $\mathbf{u}=(u_0,\ u_1,\ u_2,\ \cdots,\ u_{n-1})$ 是 C^* 中的任意一个码字，而 $\mathbf{x}=(x_0,\ x_1,\ x_2,\ \cdots,\ x_{n-1})$ 是 $V_n(\mathbf{F}_q)$ 中任意一个向量. 如果 $\mathbf{x}\in C$, 那么一定有

$$u_0x_0+u_1x_1+u_2x_2+\cdots+u_{n-1}x_{n-1}=0.$$

将 $x_0,\ x_1,\ x_2,\ \cdots,\ x_{n-1}$ 看作文字，那么上式就叫做 C 的一个*校验方程*，也说它是由 $\mathbf{u}$ 所确定的校验方程，它是 C 中码字必须适合的方程. 因为 $\dim C^*=n-k$, 所以 C 的线性无关的

校验方程的最大个数是 $n-k$，即 C 有 $n-k$ 个线性无关的校验方程，譬如 C 的校验矩阵 H 的 $n-k$ 个行向量所决定的 $n-k$ 的校验方程就是线性无关的，而 C 的任意 $n-k+1$ 个校验方程都线性相关. 显然 $V_n(\mathbf{F}_q)$ 中的向量是 C 的码字，当且仅当它适合 C 的 $n-k$ 个线性无关的校验方程.

设 $\mathbf{x}\in V_n(\mathbf{F}_q)$. 我们把 $n-k$ 维列向量 $H\mathbf{x}'$ 叫做 $\mathbf{x}$ 的校验子，那么 $\mathbf{x}$ 是 C 的一个码字，当且仅当 $\mathbf{x}$ 的校验子等于 $n-k$ 维零向量，即 $H\mathbf{x}'=\mathbf{0}'$. 这就是说 $\mathbf{x}$ 适合 H 的 $n-k$ 个行向量 $\mathbf{u}_0$, $\mathbf{u}_1$, $\mathbf{u}_2$, $\cdots$, $\mathbf{u}_{n-k-1}$ 所确定的 C 的校验方程.

当采用 q 元线性码 C 作为数字通信中的纠错码时，收方可以利用收到的字（即 $V_n(\mathbf{F}_q)$ 中的向量）的校验子来简化译码的过程. 我们先证明

定理 1 设 C 是 q 元 (n, k) 线性码，而 H 是它的一个校验矩阵，H 是个秩为 $n-k$ 的 $(n-k)\times n$ 矩阵，那么 $V_n(\mathbf{F}_q)$ 中的两个字 $\mathbf{x}$ 和 $\mathbf{y}$ 属于 C 的同一个陪集，当且仅当它们的校验子 $H\mathbf{x}'$ 和 $H\mathbf{y}'$ 相等.

证. $V_n(\mathbf{F}_q)$ 中两个向量 $\mathbf{x}$ 和 $\mathbf{y}$ 属于 C 的同一陪集，当且仅当 $\mathbf{x}-\mathbf{y}\in C$，因此当且仅当 $H(\mathbf{x}-\mathbf{y})'=\mathbf{0}$，即

$$H\mathbf{x}'-H\mathbf{y}'=0,$$

也即

$$H\mathbf{x}'=H\mathbf{y}'.$$

现在设数字通信中采用了一个 q 元 (n, k) 线性码 C 作为纠错码. 从引理 1 可知，C 的同一陪集中的字的校验子都相等，而 C 的不同陪集中的字的校验子不等. 这样，在排列 C 的译码表时，我们把 C 的码字排在第一行，而把 n 维零向量

$$\mathbf{0}=(\underbrace{0, 0, \cdots, 0}_{n\text{个}})$$

排成第一行的头一个码字（即最左一个码字）. 然后我们可以把 C 的同一陪集中的字排在同一行中，而用这一陪集中字的

校验子(根据引理 1，它们都相等)作为这一陪集的标记，并标在这一行的左端. 如果一个陪集中有一个字 $\mathbf{x}$ 的重量比这一陪集中其余的字的重量都小，我们就把 $\mathbf{x}$ 叫做这一陪集的陪集头，并把 $\mathbf{x}$ 排在 $\mathbf{0}$ 的下面，而在任一码字 $\mathbf{c}$ 的下面排上 $\mathbf{x}+\mathbf{c}$. 我们证明，这种排法符合根据极大似然译码方法来排译码表的排法. 实际上，设 $\mathbf{a}$ 是任意一个码字而 $\mathbf{a}\neq\mathbf{c}$，那么

$$\rho(\mathbf{x}+\mathbf{c},\ \mathbf{a})=\rho(\mathbf{x}+\mathbf{c}-\mathbf{a},\ \mathbf{0})>\rho(\mathbf{x},\ \mathbf{0})$$

而 $$\rho(\mathbf{x}+\mathbf{c},\ \mathbf{c})=\rho(\mathbf{x},\ \mathbf{0}).$$

因此 $\rho(\mathbf{x}+\mathbf{c},\ \mathbf{a})>\rho(\mathbf{x}+\mathbf{c},\ \mathbf{c})$，对 $\mathbf{a}\in C$ 而 $\mathbf{a}\neq\mathbf{c}$.

那么根据极大似然译码方法，当收方收到 $\mathbf{x}+\mathbf{c}$ 时，应译成 $\mathbf{c}$，所以 $\mathbf{x}+\mathbf{c}$ 应排在 $\mathbf{c}$ 的下面. 如果一个陪集中有多个字的重量相等而又都小于陪集中其余字的重量，譬如设陪集中 $\mathbf{x}$, $\mathbf{x}+\mathbf{a}_1$, $\mathbf{x}+\mathbf{a}_2$, $\cdots$, $\mathbf{x}+\mathbf{a}_{m-1}$ 的重量相等 ($\mathbf{0}$, $\mathbf{a}_1$, $\mathbf{a}_2$, $\cdots$, $\mathbf{a}_{m-1}$ 是 C 中 m 个码字)而

$\rho(\mathbf{x})<\rho(\mathbf{x}+\mathbf{a})$，对任意 $\mathbf{a}\in C$ 而 $\mathbf{a}\neq\mathbf{0}, \mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_{m-1}$，

那么这时可以证明陪集中任一字 $\mathbf{x}+\mathbf{c}$ 与 m 个码字 $\mathbf{c}$, $\mathbf{c}-\mathbf{a}_1$, $\mathbf{c}-\mathbf{a}_2$, $\cdots$, $\mathbf{c}-\mathbf{a}_{m-1}$ 的距离都相等而与其余码字 $\mathbf{a}$ 的距离 $\rho(\mathbf{x}+\mathbf{c},\ \mathbf{a})>\rho(\mathbf{x}+\mathbf{c},\ \mathbf{c})$. 根据极大似然译码方法，这时陪集中任一字 $\mathbf{x}+\mathbf{c}$ 应译成那个码字不能确定. 因此这时这个陪集中的字都应排在虚线下面. 但这时可以任选 $\mathbf{x}$, $\mathbf{x}+\mathbf{a}_1$, $\mathbf{x}+\mathbf{a}_2$, $\cdots$, $\mathbf{x}+\mathbf{a}_{m-1}$ 之一作为陪集头，譬如选 $\mathbf{x}$ 作为陪集头，并把 $\mathbf{x}$ 排在 $\mathbf{0}$ 的下面，而在码字 $\mathbf{c}$ 的下面排上 $\mathbf{x}+\mathbf{c}$.

例 考察一个码长 6 的二元线性码 C，它的校验矩阵是

$$H=\begin{pmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{pmatrix},\qquad(5)$$

那么 C 的信息位的个数是 3. C 一共含 $2^3=8$ 个码字. 按照上面介绍的办法，可以将 C 的译码表排成表 1.

表1 译码表

校验子＼码字	000000	110100	101010	011001	011110	110011	101101	000111
(1 0 0)′	100000	010100	001010	111001	111110	010011	001101	100111
(0 1 0)′	010000	100100	111010	001001	001110	100011	111101	010111
(0 0 1)′	001000	111100	100010	010001	010110	111011	100101	001111
(1 1 0)′	000100	110000	101110	011101	011010	110111	101001	000011
(1 0 1)′	000010	110110	101000	011011	011100	110001	101111	000101
(0 1 1)′	000001	110101	101011	011000	011111	110010	101100	000110
(1 1 1)′	001100	111000	100110	010101	010010	111111	100001	001011

现在我们来介绍如何利用按上面排列的译码表来译码。设发方发送一个码字 $\mathbf{c}$，而收方收到一个字 $\mathbf{r}$。先计算 $\mathbf{r}$ 的校验子 $H\mathbf{r}'$。然后到译码表中校验子的那一列里去查找那一个校验子等于 $H\mathbf{r}'$。找着以后，就在校验子等于 $H\mathbf{r}'$ 的那一行中去查找 $\mathbf{r}$ 这个字排在那个码字的下面，于是就把 $\mathbf{r}$ 译成这个码字。

我们来看这个译码方法何时正确译码，何时出现译码错误。令 $\mathbf{r}=\mathbf{c}+\mathbf{e}$。我们把 $\mathbf{e}$ 叫做传送过程中出现的**差错模式**。那么

$$H\mathbf{r}'=H(\mathbf{c}+\mathbf{e})'=H\mathbf{c}'+H\mathbf{e}'=H\mathbf{e}'.$$

因此如果 $\mathbf{e}$ 是 $\mathbf{r}$ 所属的陪集的陪集头，那么 $\mathbf{r}=\mathbf{c}+\mathbf{e}$ 在译码表中就排在 $\mathbf{c}$ 的下面，这时 $\mathbf{r}$ 就正确译成 $\mathbf{c}$。但是如果 $\mathbf{e}$ 不是 $\mathbf{r}$ 所属的陪集头，那么 $\mathbf{r}=\mathbf{c}+\mathbf{e}$ 在译码表中就不排在 $\mathbf{c}$ 的下面，这时 $\mathbf{r}$ 就不能译成 $\mathbf{c}$，因而出现译码错误。我们证明了，按这个译码方法译码，可以正确译码，当且仅当差错模式是陪集头。

这个译码方法当然比 §1 中介绍的要查整个译码表的方法工作量要小。但当 n 和 k 适当大时，这个译码方法的工作量仍是可观的。譬如对于二元 (100, 80) 线性码，需要从 2^{20} 个校验子中找出收到的字的校验子是哪一个，然后再从这个校验子的行中 2^{80} 个字中找出收到的字在哪一个码字的下面。这个工作量使用快速电子数字计算机也是难于完成的。因此为了使译码简单，就需要在线性码上再增加另外的代数结构或组合结构。然后再利用这些结构的特性来设计译码方法。

下面我们来讨论一下如何通过 q 元线性码的校验矩阵来研究它的纠错能力和检错能力。根据 §1 定理 2，它的纠错能力和检错能力由它的极小距离所确定。因此只要研究它的极小距离就行了。我们先证明

定理 2 设 C 是个 q 元线性码，那么 C 的极小重量等于 C 的极小距离.

证. 设 C 是码长 n 的 q 元线性码，那么 n 维零向量 $\mathbf{0}\in C$. 设 $\mathbf{a}=(a_0, a_1, a_2, \cdots, a_{n-1})$ 是 C 中任一不等于 $\mathbf{0}$ 的码字，那么

$$w(\mathbf{a})=\sum_{a_i\neq 0}1=\rho(\mathbf{a}, \mathbf{0}).$$

因此

$$\min\{w(\mathbf{a})\,|\,\mathbf{a}\in C, \mathbf{a}\neq\mathbf{0}\}$$
$$\geqslant\min\{\rho(\mathbf{a}, \mathbf{b})\,|\,\mathbf{a}, \mathbf{b}\in C, \mathbf{a}\neq\mathbf{b}\}.$$

另一方面，如果 $\mathbf{a}$, $\mathbf{b}$ 是 C 中任意两个码字，而 $\mathbf{a}\neq\mathbf{b}$，那么

$$\rho(\mathbf{a}, \mathbf{b})=\sum_{a_i\neq b_i}1=\sum_{a_i-b_i\neq 0}1=w(\mathbf{a}-\mathbf{b}).$$

因 C 是线性码，$\mathbf{a}-\mathbf{b}\in C$. 所以

$$\min\{\rho(\mathbf{a}, \mathbf{b})\,|\,\mathbf{a}, \mathbf{b}\in C, \mathbf{a}\neq\mathbf{b}\}$$
$$\geqslant\min\{w(\mathbf{a})\,|\,\mathbf{a}\in C, \mathbf{a}\neq\mathbf{0}\}.$$

因此

$$\min\{w(\mathbf{a})\,|\,\mathbf{a}\in C, \mathbf{a}\neq\mathbf{0}\}$$
$$=\min\{\rho(\mathbf{a}, \mathbf{b})\,|\,\mathbf{a}, \mathbf{b}\in C, \mathbf{a}\neq\mathbf{b}\}.$$

根据定理 2，要确定线性码的纠错能力和检错能力，只要确定它的极小重量就行了.

定理 3 设 C 是个 q 元线性码，H 是它的一个校验矩阵. 如果 H 的任意 t 列都线性无关，而 H 有 $t+1$ 列线性相关，那么 C 的极小重量等于 $t+1$. 这时 C 是可以检查出 t 个差错的检错码，也是可以纠正 $\left[\frac{t}{2}\right]$ 个差错的纠错码，这里

$$\left[\frac{t}{2}\right]=\begin{cases}\dfrac{t}{2}, & \text{如果 } t \text{ 是偶数},\\ \dfrac{t-1}{2}, & \text{如果 } t \text{ 是奇数}.\end{cases}$$

证. 设 $\mathbf{x}$ 是一个字，那么 $\mathbf{x}$ 是 C 的一个码字，当且仅当 $H\mathbf{x}'=\mathbf{0}'$. 因此 C 的任一码字均确定 H 的某些列之间的一个线性关系；反过来 H 的某些列之间的一个线性关系也确定 C 的一个码字. 具体说来，设 $\mathbf{c}$ 是 C 的一个码字，那么 $H\mathbf{c}'=\mathbf{0}'$. 如果 $\mathbf{c}$ 的第 i_0 分量，第 i_1 分量，第 i_2 分量，…和第 i_{k-1} 的分量都不等于 0 而其余分量都等于 0，那么 $H\mathbf{c}'=\mathbf{0}'$ 就是 H 的第 i_0 列，第 i_1 列，第 i_2 列，…和第 i_{k-1} 列之间的一个线性关系. 反过来，如果 H 的第 i_0 列，第 i_1 列，第 i_2 列，…和第 i_{k-1} 列线性相关，那么其第 i_0 分量，第 i_1 分量，第 i_2 分量，…和第 i_{k-1} 分量分别等于这个线性关系中的相应系数而余分量都等于 0 的向量 $\mathbf{c}$ 就适合条件 $H\mathbf{c}'=\mathbf{0}'$，因此 $\mathbf{c}$ 就是 C 中的码字. 这样一来，如果 H 的任意 t 列都线性无关，而 H 有 $t+1$ 列线性相关，那么 C 就不能有重量 $\leqslant t$ 的码字（即仅 $\leqslant t$ 个分量不为 0 的码字），而 C 有重量 $t+1$ 的码字. 因此 C 的极小重量等于 $t+1$.

至于本定理最后一个断言则是 §1 定理 2 和本节定理 2 的直接推论.

系理 设 C 是个二元线性码，H 是它的一个校验矩阵，那么 C 是可纠正一个差错的纠错码，当且仅当 H 没有元素全等于 0 的列而且 H 的任意两列都不相等.

在上面举的例子里，校验矩阵(5)就符合系理的条件，因此以(5)为校验矩阵的线性码是可以纠一个差错的纠错码. 这一点从译码表当然也可以直接看出来.

§3 循环码

设 C 是码长 n 的 q 元线性码. 如果当 $(c_0, c_1, c_2, \cdots, c_{n-1})$ 是 C 中码字时，$(c_{n-1}, c_0, c_1, \cdots, c_{n-2})$ 也一定是 C 中的码字，

那么 C 就叫循环码. 循环码比线性码有更多的代数结构. 这就是

定理 1 设 C 是码长 n 的 q 元循环码. 令

$$I(C)=\{c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1} \mid (c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1})\in C\},$$

那么 $I(C)$ 是环 $\mathbf{F}_q[x]_{x^n-1}$ 中的一个理想. 设 $g(x)$ 是 $I(C)$ 中任意一个次数最低的不等于 0 的多项式, 那么 $I(C)$ 是由 $g(x)$ 生成的理想而 $g(x)\mid x^n-1$. 更设 $\partial^0 g(x)=n-k$, 那么 $(c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1})\in C$, 当且仅当有一个 $\mathbf{F}_q$ 上的次数小于 k 的多项式 $k(x)$ 存在使

$$c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}=k(x)g(x).$$

写

$$g(x)=g_0+g_1x+g_2x^2+\cdots+g_{n-k}x^{n-k},\ g_0g_{n-k}\neq 0, \tag{1}$$

那么 $k\times n$ 矩阵

$$G=\left.\begin{pmatrix} g_0 & g_1 & g_2\cdots g_{n-k} & & & 0\\ & g_0 & g_1 & g_2\cdots g_{n-k} & & \\ 0 & & \ddots & & \ddots & \\ & & & g_0 & g_1 & g_2\cdots g_{n-k}\end{pmatrix}\right\}k\text{ 行}. \tag{2}$$

就是 C 的一个生成矩阵, 因此 C 是个 $(n,\ k)$ 码.

证. 定义一个从 $V_n(\mathbf{F}_q)$ 到 $\mathbf{F}_q[x]_{x^n-1}$ 之上的一一映射

$$\tau:\ (a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1})\to a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1},$$

$$\text{对任意}(a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1})\in V_n(\mathbf{F}_q).$$

$\mathbf{F}_q[x]_{x^n-1}$ 也有一个向量空间的结构, 即 $\mathbf{F}_q[x]_{x^n-1}$ 对于加法运算和用 $\mathbf{F}_q$ 中元素去乘 $\mathbf{F}_q[x]_{x^n-1}$ 中元素的运算来说是 $\mathbf{F}_q$ 上的一个 n 维向量空间. 显然 τ 是向量空间 $V_n(\mathbf{F}_q)$ 到向量空间 $\mathbf{F}_q[x]_{x^n-1}$ 的一个同构, 而

$$I(C)=\tau(C).$$

利用 C 是线性码这一点, 容易证明 $I(C)$ 是 $\mathbf{F}_q[x]_{x^n-1}$ 的子空间. 将 τ 看作从 C 到 $I(C)$ 的映射, τ 是从子空间 C 到子空

间 $I(C)$ 的一个同构.

仍设 $c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in I(C)$,

那么 $(c_0, c_1, c_2, \cdots, c_{n-1})\in C$.

因 C 是循环码,所以

$$(c_{n-1}, c_0, c_1, \cdots, c_{n-2})\in C.$$

因此

$$\begin{aligned}
&x\odot(c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1})\\
&=(c_0x+c_1x^2+c_2x^3+\cdots+c_{n-1}x^n)_{x^n-1}\\
&=c_{n-1}+c_0x+c_1x^2+\cdots+c_{n-2}x^{n-1}\in I(C),
\end{aligned}$$

对 n 用归纳法即可推出

$$x^i\odot(c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1})\in I(C),$$

$$i=0, 1, 2, \cdots, n-1.$$

因 $\mathbf{F}_q[x]_{x^n-1}$ 中任一元素都是某几个 $x^i(i=0, 1, 2, \cdots, n-1)$ 的系数属于 F_q 的线性组合. 再利用上面证明的 $I(C)$ 是个子空间这一事实即可推出,对任意 $k(x)\in\mathbf{F}_q[x]_{x^n-1}$, 都有

$$k(x)\odot(c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1})\in I(C).$$

这样根据第一章§6定理4就可知道 $I(C)$ 是 $\mathbf{F}_q[x]_{x^n-1}$ 的理想. 再根据第一章§6定理7就知道 $I(C)$ 由 $I(C)$ 中次数最低的首项系数等于1的多项式 $g_0(x)$ 生成, 而 $g_0(x)\,|\,x^n-1$. 显然 $I(C)$ 中任意一个次数最低的不等于0的多项式都可以将 $g_0(x)$ 乘以 $\mathbf{F}_q^*$ 中的一个元素得到. 因此 $I(C)$ 由其中任意一个次数最低的不等于0的多项式 $g(x)$ 生成,即

$$I(C)=\{k(x)g(x)\,|\,\partial^0k(x)<n-\partial^0g(x)\},$$

显然也有 $g(x)\,|\,x^n-1$.

设 $\partial^0g(x)=n-k$, 那么 $g(x), xg(x), x^2g(x), \cdots, x^{k-1}g(x)$ 就是 $I(C)$ 的一组基, 而它们在同构 τ 之下的原象就是 C 的一组基. 于是 G(见(2)式)就是 C 的一个生成多项式, 而 C 的信息位的个数是 k.

这样定理 1 就完全证明了.

显然 $I(C)$ 的生成多项式, 除差一个 $\mathbf{F}_q^*$ 中的元素作为因子外, 是唯一决定的. 我们把 $I(C)$ 的生成多项式叫做 C 的生成多项式, 也说 C 是由它的生成多项式生成的循环码.

定理 1 有下面这个逆定理.

定理 2 设 $g(x)$ 是 $\mathbf{F}_q[x]$ 中的一个多项式, 而 $g(x)|x^n-1$. 用 $(g(x))$ 表示 $g(x)$ 在 $\mathbf{F}_q[x]_{x^n-1}$ 中生成的理想, 即

$$(g(x))=\{k(x)g(x)\,|\,\partial^0 k(x)<n-\partial^0 g(x)\}.$$

令

$$C=\{(c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1})\,|\,(c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1})\in V_n(\mathbf{F}_q)\ \text{而}\ c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in(g(x))\},$$

那么 C 是一个码长 n 的 q 元循环码, 它的信息位的个数等于 $n-\partial^0 g(x)$.

由于这个定理的证明非常容易, 因而我们略去不证.

现在设 C 是码长 n 的 q 元循环码, $g(x)$ 是它的一个生成多项式. 根据定理 1 可知 $(c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1})\in C$, 当且仅当

$$g(x)\,|\,c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}.$$

因 $g(x)\,|\,x^n-1$, 故可令

$$h(x)=\frac{x^n-1}{g(x)}, \tag{3}$$

$h(x)$ 是个 k 次多项式, 我们把它叫做 C 的校验多项式. 显然, $(c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1})\in C$, 当且仅当

$$(h(x)\cdot(c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}))_{x^n-1}=0. \tag{4}$$

写

$$h(x)=h_0+h_1x+h_2x^2+\cdots+h_kx^k,\ h_0h_k\neq 0. \tag{5}$$

令

$$H=\left.\begin{pmatrix} h_k & h_{k-1} & \cdots & h_1 & h_0 & & & 0 \\ & h_k & h_{k-1} & \cdots & h_1 & h_0 & & \\ & & \ddots & & & & \ddots & \\ 0 & & & h_k & h_{k-1} & \cdots & h_1 & h_0 \end{pmatrix}\right\}n-k\ \text{行} \tag{6}$$

那么 H 是秩为 $n-k$ 的 $(n-k)\times n$ 矩阵. 把(3)式写成

$$g(x)h(x)=x^n-1,$$

那么就有

$$g_ih_k+g_{i+1}h_{k-1}+\cdots+g_{n-k}h_{i+2k-n}=0,\quad 0<i+k<n,\qquad (7)$$

在上式中我们约定 $h_{-1}=h_{-2}=\cdots=0$. 将(7)式写成矩阵形式就是

$$GH'=0,\qquad (8)$$

因此 H 是 C 的校验矩阵.

再注意, 因 $h(x)\,|\,x^n-1$, $h(x)$ 也是一个 q 元循环码的生成多项式. 根据上面的讨论, 以 $h(x)$ 为生成多项式的循环码的一个生成矩阵是

$$\left.\begin{pmatrix} h_0 & h_1 & h_2\cdots h_k & & & 0 \\ & h_0 & h_1 & h_2\cdots h_k & & \\ 0 & & \ddots & & \ddots & \\ & & h_0 & h_1 & h_2\cdots h_k \end{pmatrix}\right\} n-k\text{ 行},$$

将这个矩阵与(6)相比较, 可知以 $h(x)$ 为生成多项式的循环码与以 $g(x)$ 为生成多项式的循环码的对偶码是等价的. 实际上将以 $h(x)$ 为生成多项式的循环码的位置集合 $\{0, 1, 2, \cdots, n-1\}$ 改排成 $\{n-1, n-2, \cdots, 2, 1, 0\}$, 即将它的码字 $(c_0, c_1, c_2, \cdots, c_{n-1})$ 改排成 $(c_{n-1}, c_{n-2}, \cdots, c_2, c_1, c_0)$ 就是以 $g(x)$ 为生成多项式的循环码的对偶码中的码字, 而且反过来也对. 更进一步, 如果引进与 $h(x)$ 互反的多项式

$$\tilde{h}(x)=x^kh(1/x)=h_k+h_{k-1}x+h_{k-2}x^2+\cdots+h_1x^{k-1}+h_0x^k,$$

那么以 $\tilde{h}(x)$ 为生成多项式的循环码就恰好是以 $g(x)$ 为生成多项式的循环码的对偶码. 这样我们证明了

定理3 设 $g(x)$ 是 $\mathbf{F}_q[x]$ 中的一个多项式, 而 $g(x)\,|\,x^n-1$. 令 $h(x)=(x^n-1)/g(x)$, 那么以 $h(x)$ 为生成多项式的循环码与以 $g(x)$ 为生成多项式的循环码的对偶码等价. 实际上,

只要将以 $h(x)$ 为生成多项式的循环码的码字 $(c_0, c_1, c_2, \cdots, c_{n-1})$ 改排成 $(c_{n-1}, c_{n-2}, \cdots, c_1, c_0)$ 就是以 $g(x)$ 为生成多项式的循环码的对偶码的码字，而且反过来. 更进一步，以 $g(x)$ 为生成多项式的循环码的对偶码恰好是以与 $h(x)$ 互反的多项式 $\tilde{h}(x)$ 为生成多项式的循环码.

有时我们把由 $h(x)$ 生成的循环码和由与 $h(x)$ 互反的多项式 $\tilde{h}(x)$ 生成的循环码视为同一. 这样我们也可以说，当 $x^n-1=g(x)h(x)$ 时，以 $g(x)$ 为生成多项式的循环码与以校验多项式 $h(x)$ 为生成多项式的循环码互为对偶码.

循环码的编码非常简单，可以用很简单的电子设备来实现. 下面我们来阐明这一点.

设 C 是 q 元 (n, k) 循环码，$g(x)$ 是它的一个生成多项式，那么 $\partial^0 g(x)=n-k$. 将 $g(x)$ 写作(1)，那么(2)中的 G 就是 C 的一个生成矩阵. 因 $g_{n-k}\neq 0$，所以 G 行等价于以下形状的一个矩阵

$$(P_1^{(k,n-k)}, I^{(k)}).$$

因此可以把 C 中码字的后 k 位看作是信息位，而前 $n-k$ 位看作是校验位. 假定给了信息位 $c_{n-k}, c_{n-k+1}, \cdots, c_{n-1}$ 的值，它们是 $\mathbf{F}_q$ 中的元素. 问题是如何从它们唯一地定出 $c_0, c_1, c_2, \cdots, c_{n-k-1}$ 使

$$(c_0, c_1, c_2, \cdots, c_{n-k-1}, c_{n-k}, c_{n-k+1}, \cdots, c_{n-1})\in C.$$

令
$$c(x)=c_{n-k}x^{n-k}+c_{n-k+1}x^{n-k+1}+\cdots+c_{n-1}x^{n-1}.$$

根据带余除法，可以写

$$c(x)=q(x)g(x)-r(x),\quad \partial^0 r(x)<\partial^0 g(x)=n-k,$$

而且 $r(x)$ 由 $c(x)$ 和 $g(x)$ 唯一确定. 那么

$$g(x)\,|\,c(x)+r(x).$$

因此
$$c(x)+r(x)\in I(C).$$

设 $r(x)=c_0+c_1x+c_2x^2+\cdots+c_{n-k-1}x^{n-k-1}$，$c_i\in\mathbf{F}_q$.

那么 $c(x)+r(x)$ 在 τ 之下的原象

$$(c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-k-1},\ c_{n-k},\ c_{n-k+1},\ \cdots,\ c_{n-1})\in\mathcal{C}.$$

所以校验位 $c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-k-1}$ 可以由带余除法唯一地定出. 在工程上这可以用除法电路来实现.

下面是用 $g(x)=\sum_{i=0}^{n-k}g_ix^i$ 做除式的除法电路的框图:

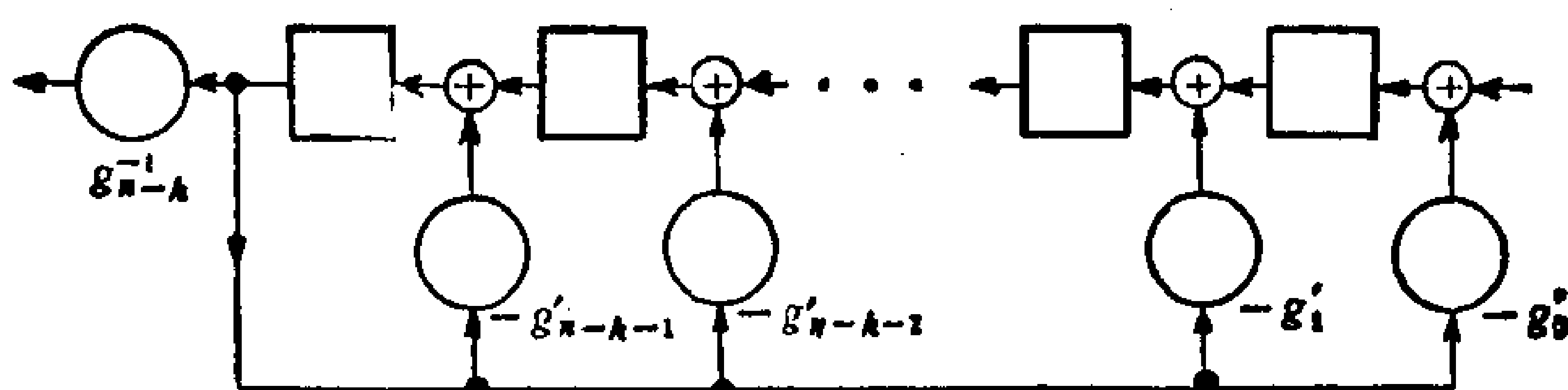


图 1

图 1 中一共有 $n-k$ 个寄存器, 而 $n-k=\partial^0 g(x)$, 每个寄存器可以取 q 种状态之一, 这 q 种状态分别用 $\mathbf{F}_q$ 里的 q 个元素来代表, 其余符号, 即加法器和乘法器, 其意义和第三章 §1 中所说的一样; 而 $g'_i=g_{n-k}^{-1}g_i(i=0,\ 1,\ 2,\ \cdots,\ n-k-1)$. 设这个除法电路中 $n-k$ 个寄存器的初始状态都是 0. 然后按移位脉冲的节拍, 从这个除法电路左方的输入端依次输入 n 个 $\mathbf{F}_q$ 中的元素

$$a_{n-1},\ a_{n-2},\ \cdots,\ a_1,\ a_0,$$

那么当 a_0 输送进去时, 这个除法电路的 $n-k$ 个寄存器的内容就是用 $g(x)$ 去除 $a(x)=\sum_{i=0}^{n-1}a_ix^i$ 所得的余式

$$r(x)=\sum_{i=0}^{n-k-1}r_ix^i$$

的系数, 从左往右依序是 $r_{n-k-1},\ r_{n-k-2},\ \cdots,\ r_1,\ r_0$. 另一方面, 从第 $n-k+1$ 个移位脉冲开始直到第 n 个移位脉冲为止, 这个除法电路左方的输出端的输出就依序是用 $g(x)$ 去除 $a(x)$ 所得的商的 $k-1$ 次项的系数, $k-2$ 次项的系数, $\cdots$, 零次项

的系数.

特别,当给定以 $g(x)$ 为生成多项式的循环码 C 的 k 个信息位的值 $c_{n-k}, c_{n-k+1}, \cdots, c_{n-1}$ 以后,按移位脉冲的节拍依次向这个除法电路的输入端输入下面这 n 个元素

$$c_{n-1}, c_{n-2}, \cdots, c_{n-k+1}, c_{n-k}, \underbrace{0, 0, \cdots, 0}_{n-k\text{个}},$$

当最后一个 0 输进去时,设这个除法电路的 $n-k$ 个寄存器的内容从左往右依序是

$$-c_{n-k-1}, -c_{n-k-2}, \cdots, c_{-1}, -c_0.$$

那么 $(c_0, c_1, \cdots, c_{n-k-1}, c_{n-k}, c_{n-k+1}, \cdots, c_{n-1})$

就是 C 的一个码字.

举一个例子. 考察以

$$g(x)=x^4+x+1$$

为生成多项式的码长 15 的二元循环码 C. 因为在 $\mathbf{F}_2[x]$ 中

$$x^4+x+1|x^{15}-1,$$

所以 C 确实是存在的, 它是个(15, 11)循环码. C 的编码可以用下面图 2 中的除法电路来实现. 当给定信息位 $c_4, c_5, \cdots, c_{14}$ 后, 先设图 2 中 4 个寄存器的初始状态都是 0, 再按移位脉冲的节拍依序输入 $c_{14}, c_{13}, \cdots, c_4, 0, 0, 0, 0$ 后,寄存器中的内容自左至右依序就是 c_3, c_2, c_1, c_0 而 $(c_0, c_1, \cdots, c_{14})$ 就是 C 的一个码字.

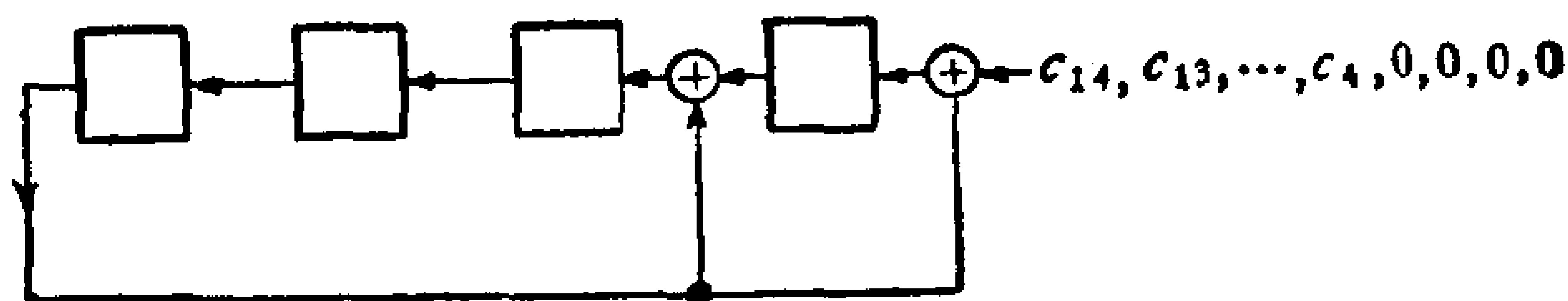


图 2

另一方面,因 $g(x)|x^n-1$, 所以 $g_0\neq0$, 于是 G 也行等价于以下形状的一个矩阵

$$(I^{(k)},\ P_2^{(k,\,n-k)}).$$

因此也可以把 C 中码字的前 k 位看作是信息位，而后 $n-k$ 位看作是校验位．假定给了 $c_0,\ c_1,\ c_2,\ \cdots,\ c_{k-1}$ 的值．问题是如何从它们唯一地定出 $c_k,\ c_{k+1},\ \cdots,\ c_{n-1}$ 使

$$(c_0,\ c_1,\ c_2,\ \cdots,\ c_{k-1},\ c_k,\ c_{k+1},\ \cdots,\ c_{n-1})\in C.$$

由(4)式知，当 $m\geqslant k$ 时有

$$h_0c_m+h_1c_{m-1}+\cdots+h_kc_{m-k}=0.$$

这就是说，在下面的 q 元 k 级线性移位寄存器中，如果初始状态是 $(c_0,\ c_1,\ c_2,\ \cdots,\ c_{k-1})$，那么它的输出的前 n 个元素就是 $c_0,\ c_1,\ c_2,\ \cdots,\ c_{k-1},\ c_k,\ c_{k+1},\ \cdots,\ c_{n-1}.$

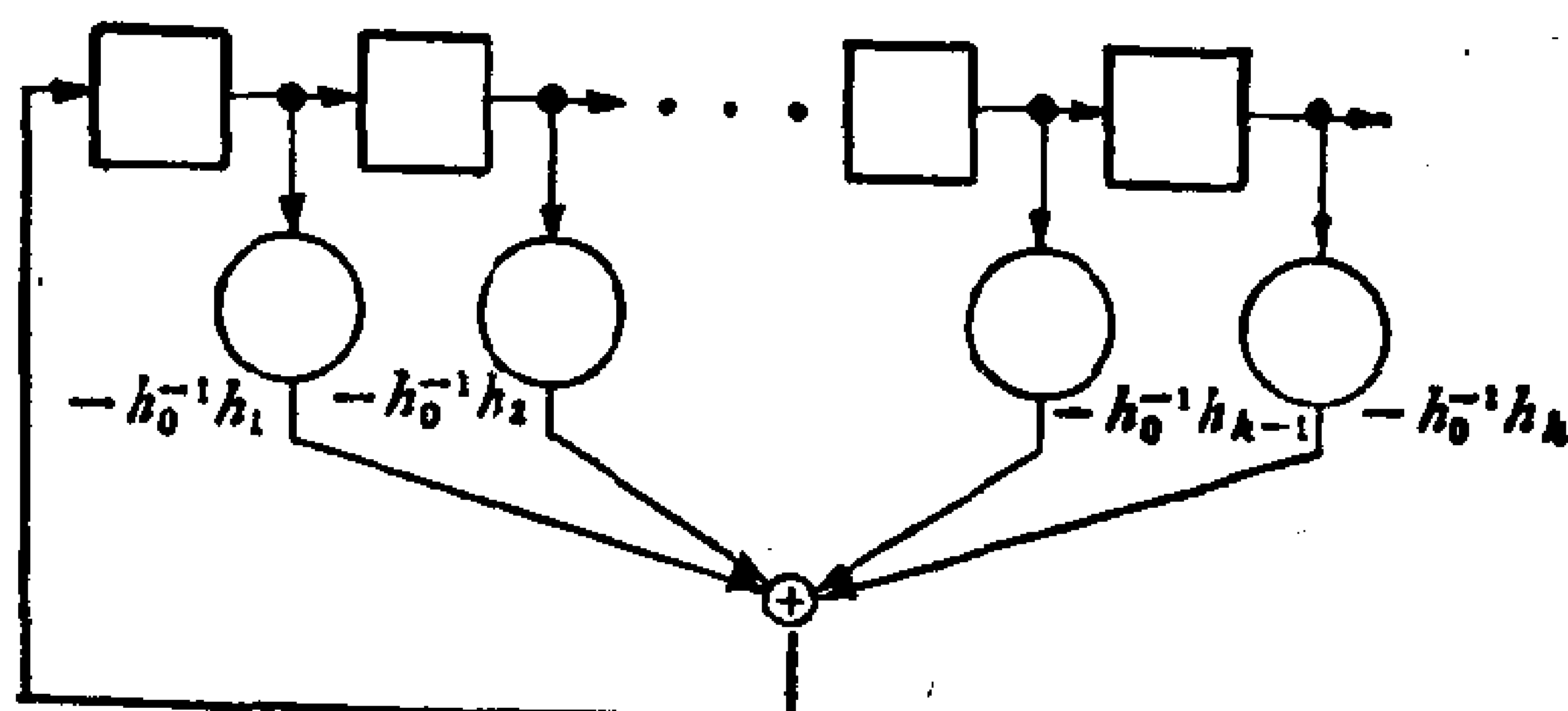


图 3

再举上面的例子来说明．我们有

$$h(x)=\frac{x^{15}-1}{x^4+x+1}=x^{11}+x^8+x^7+x^5+x^3+x^2+x+1.$$

那么当给定以 x^4+x+1 为生成多项式的二元循环码 C 的一个码字的信息位 $c_0,\ c_1,\ c_2,\ \cdots,\ c_{10}$ 之后，将它们存入下面的移位寄存器里，那么这个移位寄存器的输出的头 15 个元素就是 C 的以 $c_0,\ c_1,\ c_2,\ \cdots,\ c_{10}$ 为信息位的码字 $(c_0,\ c_1,\ c_2,\ \cdots,\ c_{10},\ c_{11},\ c_{12},\ c_{13},\ c_{14})$．注意这种编码方法需要 11 个寄存器，而上面的编码方法只需要 4 个寄存器．但当 $\partial^0h(x)<\partial^0g(x)$ 时，第二种编码方法所需要的寄存器的个数就比第一种编码方法少．

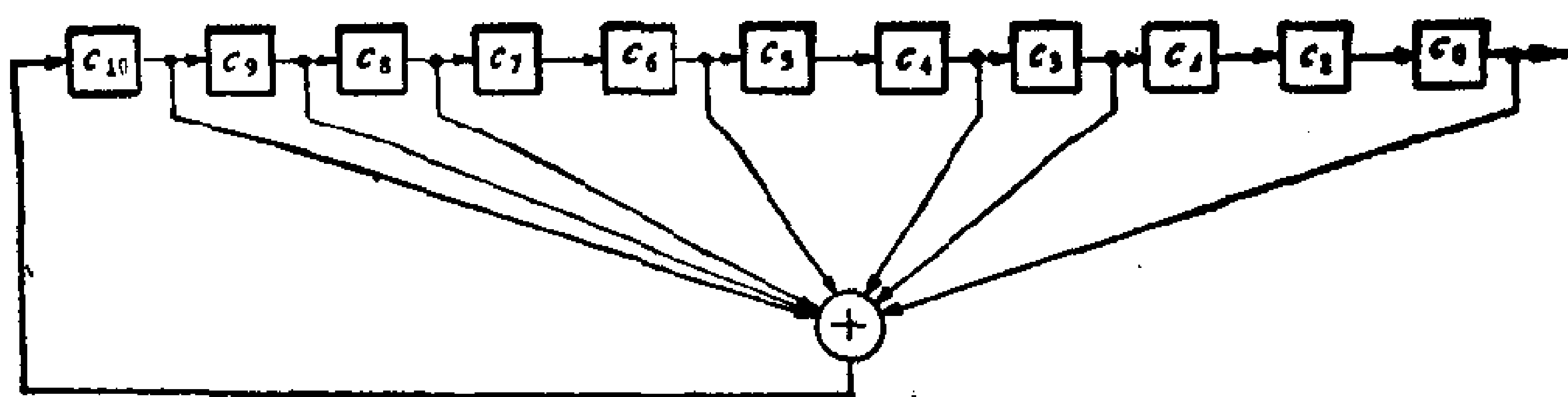


图 4

第二种编码方法启发我们去研究循环码和由它的校验多项式所产生的线性移位寄存器序列的关系.

设 $h(x)$ 是 $\mathbf{F}_q$ 上的一个零次项不等于 0 的 k 次多项式. 写

$$h(x)=h_0+h_1x+h_2x^2+\cdots+h_kx^k,\ h_0h_k\neq 0.$$

我们把 $\mathbf{F}_q$ 上的一个无限序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)$$

叫做由 $h(x)$ 产生的 q 元 k 级线性移位寄存器序列, 如果

$$h_0a_m+h_1a_{m-1}+h_2a_{m-2}+\cdots+h_ka_{m-k}=0,\quad m\geqslant k. \tag{9}$$

根据第三章 §1 定理 1, 我们知道一共有 q^k 个由 $h(x)$ 产生的 q 元 k 级线性移位寄存器序列. 我们用 $G(h)$ 来表示由 $h(x)$ 所产生的线性移位寄存器序列的全体所组成的集合. 我们也知道 $G(h)$ 是 $\mathbf{F}_q$ 上的一个 k 维向量空间, 更进一步, 我们有

定理 4 设 $h(x)$ 是 $\mathbf{F}_q$ 上的一个零次项不等于 0 的 k 次多项式, n 是 $h(x)$ 的周期的一个倍数. 对任意 $\mathbf{a}\in G(h)$, 将 $\mathbf{a}$ 的前 n 项构成的向量 $(a_0,\ a_1,\ a_2,\ \cdots,\ a_{n-1})$ 仍记作 $\mathbf{a}$, 用 $C(h)$ 来代表 $G(h)$ 中序列的前 n 项构成的向量所组成的集合. 那么 $C(h)$ 是个 $(n,\ k)$ 循环码, 并以

$$g(x)=\frac{x^n-1}{h(x)}$$

为生成多项式, 因而与 $h(x)$ 为生成多项式的循环码的对偶码等价.

证. 设 $\mathbf{a}=(a_0, a_1, a_2, \cdots)\in G(h)$,

那么 $\tau_0: \mathbf{a}\to(a_0, a_1, a_2, \cdots, a_{n-1})$

就是从 $G(h)$ 映到 $C(h)$ 之上的一个映射. 因 $\mathbf{a}$ 由它的前 k 项唯一确定, 而 $k\leqslant n$, 所以 τ_0 是从 $G(h)$ 到 $C(h)$ 的一个一一对应. 因 $G(h)$ 是 $\mathbf{F}_q$ 上的向量空间, 容易证明 $C(h)=\tau_0(G(h))$ 也是 $\mathbf{F}_q$ 上的向量空间, 而实际上 τ_0 是从 $\mathbf{F}_q$ 上的向量空间 $G(h)$ 到 $\mathbf{F}_q$ 上的向量空间 $C(h)$ 的同构. 因 $\dim G(h)=k$, 根据第二章 §1 定理 7 $\dim C(h)=k$. 因此 $C(h)$ 是 (n, k) 线性码.

根据第三章 §2 定理 1 和定理 4 的系理 3, $G(h)$ 中的序列都是周期序列, 而且它们的周期都是 $h(x)$ 的周期的因数, 因而都是 n 的因数. 我们也知道, 当 $\mathbf{a}=(a_0, a_1, a_2, \cdots)\in G(f)$ 时, $(a_1, a_2, a_3, \cdots)$ 也属于 $G(f)$. 利用这些性质就立刻可以推出 $C(h)$ 是循环码.

剩下来还需要证明 $C(h)$ 以 $g(x)$ 为生成多项式. 由 (9) 式可知 $C(h)$ 以 H (见 (6) 式) 为校验矩阵. 因 $g(x)h(x)=x^n-1$, 所以 (8) 式成立. 于是 $C(h)$ 以 G 为生成矩阵. 因此 $C(h)$ 以 $g(x)$ 为生成多项式. 再根据定理 3 可知 $C(h)$ 与以 $h(x)$ 为生成多项式的循环码的对偶码等价.

这证明了定理 4.

反过来, 我们有

定理 5 设 C 是 $\mathbf{F}_q$ 上的一个 (n, k) 循环码, 以 $g(x)$ 为生成多项式, $\partial g^0(x)=n-k$. 令

$$h(x)=\frac{x^n-1}{g(x)},$$

那么 $C=C(h)$.

这是定理 4 的直接推论, 它是上面介绍的循环码的第二种编码方法的根据.

特别，当 $h(x)$ 是 $\mathbf{F}_q$ 上的 r 次本原多项式时，$G(h)$ 中非零序列的周期都等于 q^r-1，即都是m序列. 用 $C(h)$ 表 $G(h)$ 中序列的前 q^r-1 项构成的向量所组成的 q 元 (q^r-1, r) 循环码，即 $C(h)$ 是所有由 $h(x)$ 产生的 m 序列的一个周期所构成的 q^r-1 个向量再加上 q^r-1 维零向量所组成的(q^r-1, r)循环码. 我们把 $C(h)$ 叫做码长 q^r-1 的 q 元*m序列码*. 从定理 4 立刻推出

定理 6 设 $h(x)$ 是 $\mathbf{F}_q$ 上的 r 次本原多项式，那么码长 q^r-1 的 q 元m序列码 $C(h)$ 以 $x^{q^r-1}-1/h(x)$ 为生成多项式，并与以 $h(x)$为生成多项式的循环码的对偶码等价，因而也就是以与 $h(x)$ 为互反多项式的 $\tilde{h}(x)$ 为生成多项式的循环码的对偶码.

最后我们再作两个注记.

(1) 根据定理 1 和定理 2，求码长 n 的所有 q 元循环码的问题，等于求它的生成多项式 $g(x)$的问题，而 $g(x)\,|\,x^n-1$. 因此要求出所有码长 n 的循环码，只要求出 x^n-1 的所有因式即可. 要解决后面这个纯代数问题，就需要把 x^n-1 在 $\mathbf{F}_q$ 上分解成不可约多项式的乘积就行了. 这个问题将在第五章中讨论.

(2) 尽管循环码的编码可以很简单地实现，但是循环码的译码器往往要根据选定的循环码的特殊结构来设计.

§4 Hamming 码

设 C 是个二元 $(n, n-r)$ 线性码，那么它的校验矩阵 H 是个秩为 r 的 $r\times n$ 矩阵. 根据 §2 定理 3 的系理我们知道，C 是可纠正一个差错的纠错码，当且仅当 H 没有元素全等于 0 的列而且 H 的任意两列都不相等. 因此为了得到可纠正一

个差错的二元 $(n, n-r)$ 线性纠错码，只要从 $\mathbf{F}_2$ 上的 r 维非零列向量中选出 n 个来，譬如是 $\mathbf{h}'_0, \mathbf{h}'_1, \mathbf{h}'_2, \cdots, \mathbf{h}'_{n-1}$，并把它们按任意次序排成一个 $r\times n$ 矩阵，譬如

$$H=(\mathbf{h}'_0, \mathbf{h}'_1, \mathbf{h}'_2, \cdots, \mathbf{h}'_{n-1}).$$

只要 H 的秩等于 r，那么以 H 为校验矩阵的二元 $(n, n-r)$ 线性码 C 就是一个可以纠正一个差错的码. 因 $\mathbf{F}_2$ 上一共有 2^r-1 个 r 维非零列向量，所以一定有 $n\leqslant 2^r-1$. 二元 $(n, n-r)$ 线性码 C 的信息位的个数是 $n-r$，它的信息率就等于 $\frac{n-r}{n}=1-\frac{r}{n}$. 因此，当 r 给定后，码愈长，信息率就愈高. 而当 $n=2^r-1$ 时，信息率达到极大值 $1-\frac{r}{2^r-1}$. 这时 H 是以 $\mathbf{F}_2$ 上 2^r-1 个非零列向量作为列向量构成的 $r\times(2^r-1)$ 矩阵. 这个矩阵的秩显然是 r，以它为校验矩阵的二元 $(2^r-1, 2^r-1-r)$ 线性码就叫做二元 $(2^r-1, 2^r-1-r)$Hamming码，简称 Hamming 码. 又因 $\mathbf{F}_2$ 上 2^r-1 个 r 维非零列向量都在 Hamming 码的校验矩阵中出现，所以校验矩阵的任意两个列向量的和是另一个列向量，因此 Hamming 码的校验矩阵有 3 个列线性相关，根据 §2 定理3，Hamming 码的极小重量等于 3.

我们证明了

定理 1 二元 $(2^r-1, 2^r-1-r)$Hamming 码是能纠正一个差错的线性码，而且是能纠正一个差错的校验位的个数等于 r 的二元线性码中信息率最大的码；它的极小重量等于 3.

自然，$\mathbf{F}_2$ 上 2^r-1 个非零列向量在 Hamming 码的校验矩阵中排列的次序不同，得到的 Hamming 码可以不同，但是这些 Hamming 码是等价的，因此我们对它们不加区别. 通常有两种排列 H 的列向量的方法最为常见，我们先介绍第一

种方法. 这种方法是先把 1 与 2^r-1 之间的整数 $j(1\leqslant j\leqslant 2^r-1)$ 表成二进位数:

$$j=j_0+j_1 2+j_2 2^2+\cdots+j_{r-1}2^{r-1}, \tag{1}$$

其中 $j_0, j_1, j_2, \cdots, j_{r-1}=0$ 或 1, 那么由 j 的二进位数表示(1)就确定 $\mathbf{F}_2$ 上的一个 r 维非零列向量

$$\begin{pmatrix} j_0 \\ j_1 \\ j_2 \\ \vdots \\ j_{r-1} \end{pmatrix}.$$

通常我们取由 j 的二进位数表示所确定的 $\mathbf{F}_2$ 上的 r 维列向量作为校验矩阵 H 的第 $j-1$ 列 ($j=1, 2, \cdots, 2^r-1$). 注意, 我们把 H 的列依序叫做第 0 列, 第 1 列, 第 2 列, $\cdots$, 第 2^r-2 列. 例如, 当 $r=4$ 时, (15, 11) Hamming 码的校验矩阵是

$$H=\begin{pmatrix} 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \end{pmatrix}.$$

现在介绍排列 Hamming 码的校验矩阵 H 的列向量的第二种方法. 这个方法是非常重要的. 设 α 是域 $\mathbf{F}_{2^r}$ 中的一个本原元, 即 $\mathbf{F}_{2^r}$ 的乘法群 $\mathbf{F}_{2^r}^*$ 的一个生成元. 我们知道, $1, \alpha, \alpha^2, \cdots, \alpha^{r-1}$ 组成 $\mathbf{F}_{2^r}$ 在 $\mathbf{F}_2$ 上的一组基. 这时任一 $\alpha^j(0\leqslant j\leqslant 2^r-2)$ 可以唯一地表成 $1, \alpha, \alpha^2, \cdots, \alpha^{r-1}$ 的线性组合, 而系数属于 $\mathbf{F}_2$:

$$\alpha^j=\sum_{i=0}^{r-1} a_{ij}\alpha^i, \quad 0\leqslant j\leqslant 2^r-2. \tag{2}$$

这样 α^j 就确定了 $\mathbf{F}_2$ 上的一个 r 维非零列向量:

$$\begin{pmatrix} a_{0j} \\ a_{1j} \\ a_{2j} \\ \vdots \\ a_{r-1j} \end{pmatrix}.$$

我们通常取 α^j 所确定的 $\mathbf{F}_2$ 上的 r 维列向量作为 H 的第 j 列 $(j=0, 1, 2, \cdots, 2^r-2)$. 于是

$$H=\begin{pmatrix} a_{00} & a_{01} & a_{02} & \cdots & a_{02^r-2} \\ a_{10} & a_{11} & a_{12} & \cdots & a_{12^r-2} \\ a_{20} & a_{21} & a_{22} & \cdots & a_{22^r-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{r-10} & a_{r-11} & a_{r-12} & \cdots & a_{r-12^r-2} \end{pmatrix}. \tag{3}$$

我们也往往把 H 简记作

$$H=((\alpha^0), (\alpha^1), (\alpha^2), \cdots, (\alpha^{2^r-2})), \tag{4}$$

其中

$$(\alpha^j)=\begin{pmatrix} a_{0j} \\ a_{1j} \\ a_{2j} \\ \vdots \\ a_{r-1j} \end{pmatrix}.$$

这样一来,如果 $\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{2^r-2})$ 是 $(2^r-1, 2^r-1-r)$ Hamming 码的一个码字,那么 $H\mathbf{c}'=\mathbf{0}'$, 即

$$c_0(\alpha^0)+c_1(\alpha^1)+c_2(\alpha^2)+\cdots+c_{2^r-2}(\alpha^{2^r-2})=\mathbf{0}'.$$

上式实际上是 r 个线性关系式, 把它们依序叫做第 0 个, 第 1 个, 第 2 个, $\cdots$, 第 $r-1$ 个. 将第 0 个线性关系式乘以 α^0, 将第 1 个乘以 α^1, 将第 2 个乘以 α^2, $\cdots$, 将第 $r-1$ 个乘以 α^{r-1}, 然后再将它们相加; 注意到(2), 就有

$$c_0+c_1\alpha+c_2\alpha^2+\cdots+c_{2^r-2}\alpha^{2^r-2}=0. \tag{5}$$

反过来,如果(5)式成立,那么利用(2)式就有

$$c_0(\alpha^0)+c_1(\alpha^1)+c_2(\alpha^2)+\cdots+c_{2^r-2}(\alpha^{2^r-2})=\mathbf{0}',$$

即 $$H(c_0,\ c_1,\ c_2,\ \cdots,\ c_{2^r-2})'=0'.$$

这就是说$(c_0,\ c_1,\ c_2,\ \cdots,\ c_{2^r-2})$是$(2^r-1,\ 2^r-1-r)$Hamming码的一个码字. 我们证明了: $(c_0,\ c_1,\ c_2,\ \cdots,\ c_{2^r-2})$ 是二元$(2^r-1,\ 2^r-1-r)$Hamming 码的一个码字, 当且仅当(5)式成立. 因此我们往往把校验矩阵(4)就简记作

$$H=(1,\ \alpha,\ \alpha^2,\ \cdots,\alpha^{2^r-2}), \tag{6}$$

相应于 H 的上述表示法, 我们往往把 Hamming 码中码字的第 i 位叫做 α^i 位$(0\leqslant i\leqslant 2^r-2)$.

用 C 表示二元$(2^r-1,\ 2^r-1-r)$Hamming 码, 其校验矩阵是(6). 如果$(c_0,\ c_1,\ c_2,\ \cdots,\ c_{2^r-2})\in C$, 那么

$$c_0+c_1\alpha+c_2\alpha^2+\cdots+c_{2^r-2}\alpha^{2^r-2}=0.$$

将上式乘以 α, 并注意到 $\alpha^{2^r-1}=1$, 就有

$$c_{2^r-2}+c_0\alpha+c_1\alpha^2+\cdots+c_{2^r-3}\alpha^{2^r-2}=0.$$

这就是说$(c_{2^r-2},\ c_0,\ c_1,\ \cdots,\ c_{2^r-3})\in C$. 因此 C 是循环码.

我们有

定理 2 设 α 是 $\mathbf{F}_{2^r}$ 的一个本原元, 那么以(6)为校验矩阵的二元$(2^r-1,\ 2^r-1-r)$Hamming 码是循环码, 而且它的生成多项式是 α 在 $\mathbf{F}_2$ 上的极小多项式.

证. 用 C 表示以(6)为校验矩阵的二元$(2^r-1, 2^r-1-r)$Hamming 码. 唯一还需要证明的是 C 的生成多项式是 α 的极小多项式. 用 $g(x)$ 表 C 的生成多项式, 用 $f(x)$ 表 α 的极小多项式. 因 α 是 $\mathbf{F}_{2^r}$ 的一个本原元, 所以 $f(x)$是 r 次不可约多项式(实际上还是本原多项式). 写

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_rx^r,\ a_r=1.$$

因 $f(\alpha)=0$, 所以

$$a_0+a_1\alpha+a_1\alpha^2+\cdots+a_r\alpha^r=0.$$

因此 $$(a_0,\ a_1,\ a_2,\ \cdots,\ a_r,\ \underbrace{0,\ 0,\ \cdots,\ 0}_{2^r-2-r})\in C.$$

因 $g(x)$ 是 C 的生成多项式，所以

$$g(x) \mid f(x).$$

但 $f(x)$ 不可约，所以 $f(x)=g(x)$.

系理 设 α 是 $\mathbf{F}_{2^r}$ 的一个本原元，那么以(6)为校验矩阵的二元 $(2^r-1,\ 2^r-1-r)$ Hamming 码的对偶码就是码长 2^r-1 的 m 序列码.

证. 设 $g(x)$ 是 α 在 $\mathbf{F}_{2^r}$ 上的极小多项式，那么 $g(x)$ 是 $\mathbf{F}_{2^r}$ 上的本原多项式，而以(6)为校验矩阵的二元 Hamming 码以 $g(x)$ 为生成多项式. 根据 § 3 定理 6，它的对偶码就是

$$h(x)=\frac{x^{2^r-1}-1}{\tilde{g}(x)}$$

其中 $r=\partial^0 g(x)$，生成的码长 2^r-1 的 m 序列码.

我们举一个二元 Hamming 码的例子. 考察 $r=4$ 的情形. 先求 $\mathbf{F}_{2^4}$ 的一个本原元. 首先，考察 $\mathbf{F}_2$ 上的 4 次多项式 x^4+x+1. 因 x^4+x+1 不被 $\mathbf{F}_2$ 上的 1 次多项式 x, $x+1$ 和唯一的 2 次不可约多项式 x^2+x+1 所整除，所以 x^4+x+1 是 $\mathbf{F}_2$ 上的不可约多项式. 那么

$$x^4+x+1 \mid x^{2^4}-x.$$

于是 x^4+x+1 在 $\mathbf{F}_{2^4}$ 中有 4 个不同的根. 设其中之一是 α，即

$$\alpha^4+\alpha+1=0.$$

经简单计算可得

$\alpha^0=1,$ $\alpha^1=\alpha,$ $\alpha^2=\alpha^2,$

$\alpha^3=\alpha^3,$ $\alpha^4=1+\alpha,$ $\alpha^5=\alpha+\alpha^2,$

$\alpha^6=\alpha^2+\alpha^3,$ $\alpha^7=1+\alpha+\alpha^3,$ $\alpha^8=1+\alpha^2,$

$\alpha^9=\alpha+\alpha^3,$ $\alpha^{10}=1+\alpha+\alpha^2,$ $\alpha^{11}=\alpha+\alpha^2+\alpha^3,$

$\alpha^{12}=1+\alpha+\alpha^2+\alpha^3,$ $\alpha^{13}=1+\alpha^2+\alpha^3,$ $\alpha^{14}=1+\alpha^3,$

$\alpha^{15}=1.$

因此 α 是 $\mathbf{F}_{2^4}$ 的一个本原元. 那么 (15, 11) Hamming 码的校验阵 H 可排成

$$H=\begin{pmatrix}1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\0&0&0&1&0&0&1&1&0&1&0&1&1&1&1\end{pmatrix},$$

也可简记作

$$H=(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}).$$

二元$(2^r-1,\ 2^r-1-r)$Hamming 码 C 的校验矩阵 H 的第二种排列法(6)显示了 C 是循环码，这给 C 的编码和译码带来方便. 关于循环码的编码，在工程上可以用除法电路或线性移位寄存器来实现，这在 §3 中已作详细说明，并举了以 x^4+x+1 为生成多项式的 (15, 11)Hamming 码的编码作为例子，我们在此不再重复. 下面介绍 Hamming 码 C 的译码方法和译码器的设计.

设发方发送的码字是

$$\mathbf{c}=(c_0,\ c_1,\ c_2,\ \cdots,\ c_{2^r-2}),$$

而收方收到的字是

$$\mathbf{r}=(r_0,\ r_1,\ r_2,\ \cdots,\ r_{2^r-2}),$$

那么传输过程中出现的差错模式就是

$$\mathbf{e}=\mathbf{r}-\mathbf{c}.$$

记

$$\mathbf{e}=(e_0,\ e_1,\ e_2,\ \cdots,\ e_{2^r-2}).$$

假定传输过程中顶多有一位出现差错，即顶多有一个码元被传错，那么 $\mathbf{e}$ 的分量中顶多有一个是 1，其余都等于 0. 译码的第一步是计算收到的字 $\mathbf{r}$ 的校验子 $\mathbf{s}'=H\mathbf{r}'$，然后根据校验子 $\mathbf{s}'=H\mathbf{r}'$ 来决定应该把 $\mathbf{r}$ 译成哪个码字.

如果 $\mathbf{s}'=H\mathbf{r}'=\mathbf{0}'$，$\mathbf{r}$ 就是一个码字，那么就把 $\mathbf{r}$ 译成 $\mathbf{r}$. 倘若假定码字在信道传输过程中产生差错的个数 $\leqslant 1$，这时

一定有 $\mathbf{r}=\mathbf{c}$, 因此译码正确.

如果 $\mathbf{s}'=H\mathbf{r}'\neq\mathbf{0}'$, 那么因为 H 的 2^r-1 个列是两两不同的 2^r-1 个非零 r 维列向量, 所以 $\mathbf{s}'$ 就等于 H 的某一列. 如果将 H 写成形状(6), 那么 $\mathbf{s}'=(\alpha^i)$ 对某一个 i 而 $0\leqslant i\leqslant 2^r-2$. 显然

$$H\mathbf{e}'=H(\mathbf{r}-\mathbf{c})'=H\mathbf{r}'-H\mathbf{c}'=H\mathbf{r}'=\mathbf{s}'.$$

因此 $H\mathbf{e}'=(\alpha^i)$. 倘若假定码字在信道传输过程中产生差错的个数 $\leqslant 1$, 那么 $\mathbf{e}$ 的分量中顶多有一个是 1 而其余的是 0, 于是从 $H\mathbf{e}'=(\alpha^i)$ 就可判断

$$e_i=1,$$

$$e_j=0,\ 对\ j\neq i.$$

这就是说, $\mathbf{c}$ 在信道传输过程中, α^i 位出了差错, 因而错成 $\mathbf{r}$. 那么在译码时将 $\mathbf{r}$ 的 α^i 位改变(即如果 r_i 是 1 就改成 0, 如果 r_i 是 0 就改成 1), 而保持其他各位不动, 就能将 $\mathbf{r}$ 正确地译成发方发送的码字 $\mathbf{c}$.

现在来介绍译码器的设计, 仍举以 x^4+x+1 为生成多项式的二元 (15, 11) Hamming 码为例. 首先, 计算收到的字 $\mathbf{r}$ 的校验子 $\mathbf{s}'=H\mathbf{r}'$ 可以用以 x^4+x+1 做除式的除法电路来实现. 图 1 是以 x^4+x+1 做除式的除法电路的框图.

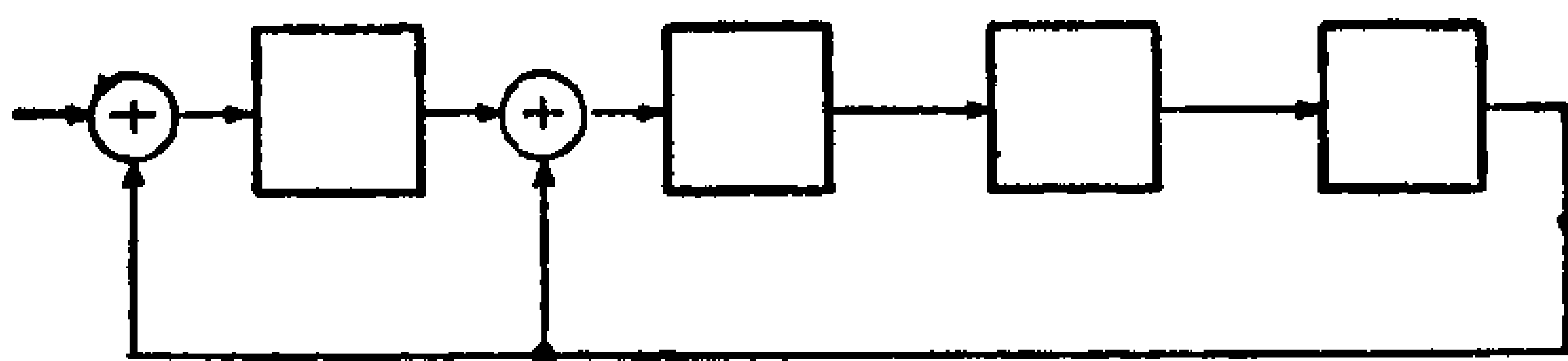


图 1

先将这个除法电路的 4 个寄存器的初始状态都置以 0, 再将 r_{14}, r_{13}, $\cdots$, r_2, r_1, r_0 按移位脉冲的节拍依序输入这个除法电路的输入端. 最后当 r_0 输进去时, 设这个除法电路的 4 个寄存器的状态从左往右依序是 s_0, s_1, s_2, s_3, 那么就有

$$\mathbf{s}' = H\mathbf{r}' = (s_0, s_1, s_2, s_3)'.$$

这就算出了校验子 $\mathbf{s}' = H\mathbf{r}'$. 令 $s = s_0 + s_1\alpha + s_2\alpha^2 + s_3\alpha^3$.

为了纠错译码，还需要一个将 $\mathbf{F}_{2^4}$ 中任一元素乘以 α 的电路. 图 2 是这样一个电路的框图. 设 $s = s_0 + s_1\alpha + s_2\alpha^2 + s_3\alpha^3$ 是 $\mathbf{F}_{2^4}$ 中的一个元素，开始时将这个电路里的 4 个寄存器从左往右依序置以 s_0, s_1, s_2, s_3，这相应于 $\mathbf{F}_{2^4}$ 中的元素 $s_0 + s_1\alpha + s_2\alpha^2 + s_3\alpha^3 = s$，我们就说这个电路的状态是 (s_0, s_1, s_2, s_3)，也说是 s. 那么加一个移位脉冲之后，这个电路的状态就是 $(s_3, s_0 + s_3, s_1, s_2)$，它相应于 $\mathbf{F}_{2^4}$ 中的元素 $s_3 + (s_0 + s_3)\alpha + s_1\alpha^2 + s_2\alpha^3 = s\alpha$，因而这个电路的状态也可以说是 $s\alpha$. 再加一个移位脉冲之后，这个电路的状态就是 $s\alpha^2$. 一般说来，设这个电路的初始状态是 s，那么加 j 个移位脉冲后，这个电路的状态就是 $s\alpha^j$.

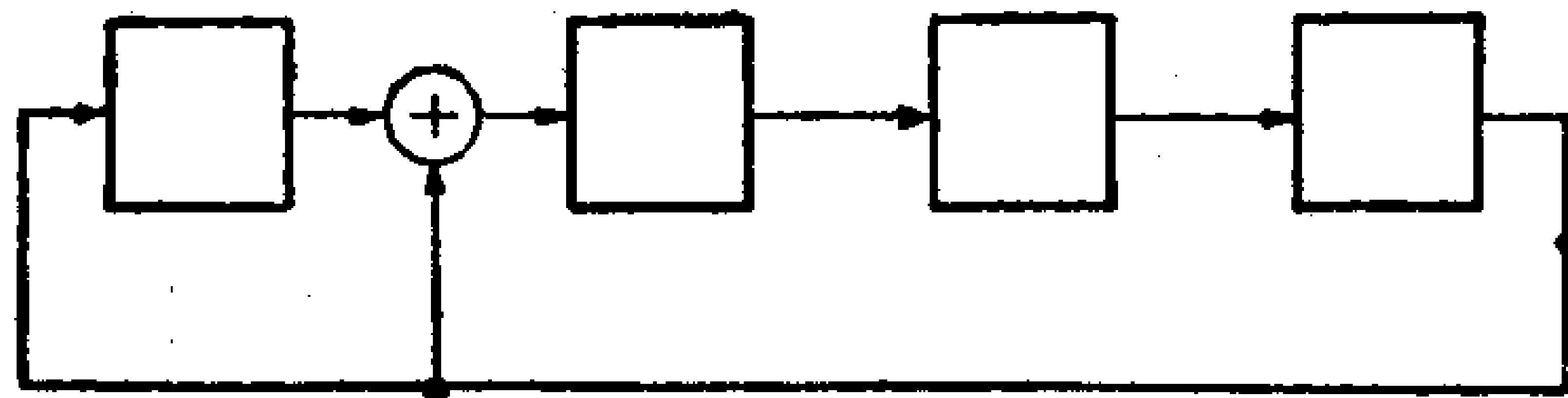
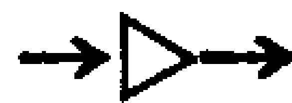


图 2

有了以上这些准备，可以如下地设计 (15, 11) Hamming 码的译码器. 它由三个移位寄存器组成，最顶上的一个由 15 个寄存器组成，下面的两个各由 4 个寄存器组成. 图 4 中



代表非门，即输入是 1 时输出是 0，而输入是 0 时输出是 1；而

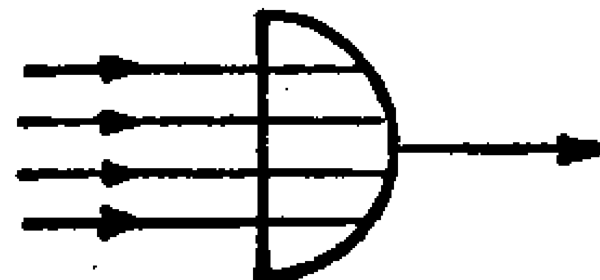


图 3

代表 4 个输入端的或门，即任意一个输入是 1 时输出都是 1，只有 4 个输入都是 0 时输出才是 0. 开始时，将顶上

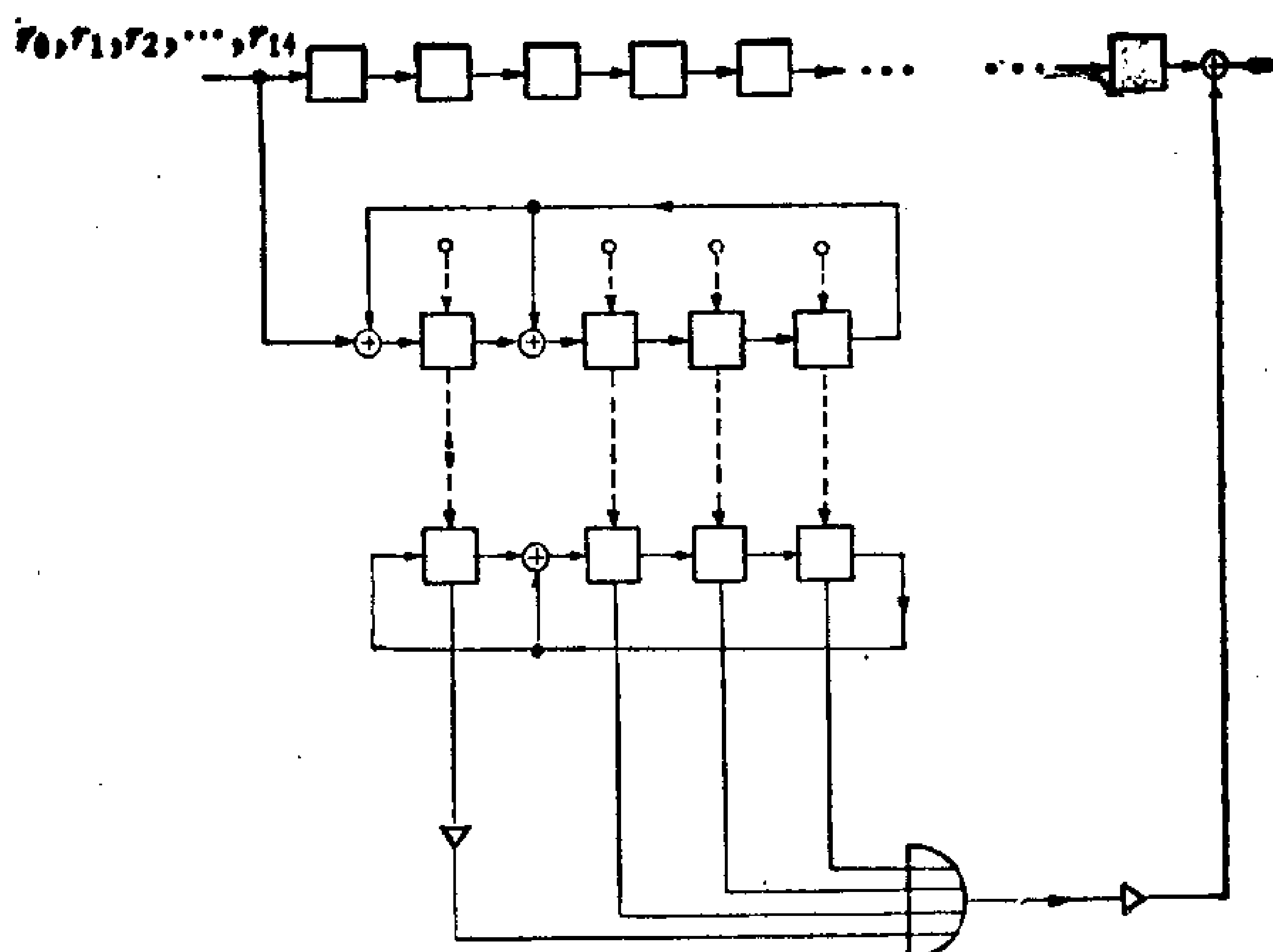


图 4 (15, 11)Hamming 码的译码器

的和中间的这两个移位寄存器的各级都置以 0, 然后将收到的字的 15 个分量 r_{14}, r_{13}, $\cdots$, r_2, r_1, r_0 按移位脉冲的节拍输入头两个移位寄存器. 当 r_0 输进去时, 顶上的移位寄存器的状态从左到右依序是 r_0, r_1, r_2, $\cdots$, r_{13}, r_{14}, 中间的移位寄存器的状态从左到右依序是 $\mathbf{r}$ 的校验子 $\mathbf{s}'=H\mathbf{r}'=(s_0,\ s_1,\ s_2,\ s_3)'$ 的系数 s_0, s_1, s_2, s_3. 这时将中间的移位寄存器的状态立刻转移给下面的移位寄存器(图中用虚线表示)并将中间的移位寄存器的状态全置以 0(图中也用虚线表示)好准备接收收到的下一个字, 当再加一个移位脉冲时, 输给顶上一排的模 2 加法器的有顶上一排最右一个寄存器的输出 r_{14}, 还有由最下面的移位寄存器来的输出, 它是 0 或 1 根据 $1+s\neq0$ 或 $=0$ 而定. 一般地, 加 j 个移位脉冲时, 输给顶上一排的模 2 加法器的有从顶上一排移位寄存器来的 r_{15-j} 和由最下面移位寄存器来的输出, 它是 0 或 1 根据 $1+s\alpha^j\neq0$ 或 $=0$ 而定. 设 $s=\alpha^i$, 即 $\mathbf{r}$ 的 α^i 位 r_i 是错的. 那么只有在 $j=15-i$ 时, $1+s\alpha^j=0$. 这就是说只有在加 $15-i$ 个脉冲时, 最下面的移

位寄存器输给顶上的模 2 加法器的才是 1，其余情形都是 0. 因此，只有在顶上的一排移位寄存器将 r_i 输给模 2 加法器时，模 2 加法器的输出是 r_i+1. 这就是当 $r_{14}, r_{13}, \cdots, r_2, r_1, r_0$ 依序通过模 2 加法器时，只有错的 α^i 位的分量 r_i 被改正，其余的 $r_j(j\neq i)$ 保持不变. 又当 $s=0$ 时，显然当 $r_{14}, r_{13}, \cdots, r_2, r_1, r_0$ 依序通过模 2 加法器时，都不改变. 因此最顶上一排模 2 加法器的输出就是应将收到的字 $\mathbf{r}$ 译成的码字.

二元 $(2^r-1, 2^r-1-r)$ Hamming 码 C 的校验矩阵的第二种排列法(6)除了给它的编码和译码带来方便以外，还启示了人们引进纠正 t 个差错的 BCH 码. 关于这后一点，将在下一节中讨论.

现在仍设 C 是 $(2^r-1, 2^r-1-r)$Hamming 码. 这时 C 的校验矩阵(6)没有分量都等于 0 的列，而且它的 2^r-1 个列也两两不同. 设

$$\mathbf{e}_i=(0, 0, \cdots, 0, \underset{\substack{\alpha^i\\ 位}}{1}, 0, \cdots, 0), \quad i=0, 1, 2, \cdots, 2^r-2$$

是 α^i 位等于 1 而其余各位都等于 0 的 n 维行向量，那么 $w(\mathbf{e}_i)=1$ 而 $H\mathbf{e}_i'=(\alpha^i)$. 因此 $V_{2^r-1}(\mathbf{F}_2)$ 中 2^r-1 个重量 1 的向量 $\mathbf{e}_i(i=0, 1, 2, \cdots, 2^r-2)$的校验子两两不同，所以它们属于 C 的不同的陪集. 这 2^r-1 个陪集再加上 C 本身就一共是 2^r 个陪集. 因为 $|C|=2^{2^r-1-r}$，所以每个陪集都含 2^{2^r-1-r} 个向量. 这样这 2^r 个陪集就总共含

$$2^r\cdot 2^{2^r-1-r}=2^{2^r-1}$$

个向量，它们就是 $V_{2^r-1}(\mathbf{F}_2)$ 的全部向量.

基于上面的分析，我们给出下面这个定义.

定义 1 设 C 是码长 n 的 q 元线性码，并假定 C 是可以纠正 t 个差错的码，那么所有重量 $\leqslant t$ 的差错模式都分属于

C 的不同的陪集. 如果所有重量 $\leqslant t$ 的差错模式所属的 C 的陪集的并正好是 $V_n(\mathbf{F}_q)$，那么 C 就叫完全码. 换句话说，如果 C 的每个陪集中都含有一个而且唯一的一个重量 $\leqslant t$ 的差错模式，C 就叫完全码.

根据定义 1 和上面的分析，我们有

定理 3 二元 $(2^r-1, 2^r-1-r)$ Hamming 码是完全码.

二元 Hamming 码有多种方法推广成 q 元码. 下面我们介绍一种推广，这种推广可以得到一个 q 元完全码.

设 q 是一个素数的幂，而 r 是个大于 1 的整数. 从 $\mathbf{F}_q$ 上的 q^r-1 个 r 维非零列向量中选出头一个分量等于 1 的来. 这样一共有 $(q^r-1)/(q-1)$ 个 r 维非零列向量. 将这 $(q^r-1)/(q-1)$ 个 r 维非零列向量排成一个 $r\times\dfrac{q^r-1}{q-1}$ 矩阵，以这个矩阵为校验矩阵的 q 元 $\left(\dfrac{q^r-1}{q-1}, \dfrac{q^r-1}{q-1}-r\right)$ 线性码就叫 q 元 Hamming 码. 完全和二元 Hamming 码一样，可以证明 q 元 Hamming 码的极小重量等于 3，因而是可以纠正一个差错的纠错码. 也可以证明 q 元 Hamming 码是完全码. 由于证明都和二元 Hamming 码的情形完全一样，我们就不重复了.

对于一般的 q 元码，即不一定是线性码的 q 元码，甚至码元取自任一含 q 个字母的字母集 Q 的 q 元码，我们可以如下地来定义完全码.

定义 2 设 Q 是一个含 q 个字母（或元素）的字母集，q 是任意一个正整数. 令

$$Q^n=\{(a_1, a_2, \cdots, a_n)\,|\,a_1, a_2, \cdots, a_n\in Q\},$$

那么 $|Q^n|=q^n$. 我们把 Q^n 叫做字的集合，而把 Q^n 的子集叫做码长 n 的 q 元码. 可以在 Q^n 中引进 Hamming 距离. 设

$\mathbf{a}=(a_1, a_2, \cdots, a_n)$, $\mathbf{b}=(b_1, b_2, \cdots, b_n)\in Q^n$. 令

$$\rho(\mathbf{a}, \mathbf{b})=\sum_{a_i\neq b_i}1.$$

我们把 $\rho(\mathbf{a}, \mathbf{b})$ 叫做 $\mathbf{a}$ 和 $\mathbf{b}$ 的 Hamming 距离. 现在设 C 是一个码长等于 n 的 q 元码, 并假定 C 是可以纠正 t 个差错的纠错码. 设 $\mathbf{c}\in C$, 令

$$S_t(\mathbf{c})=\{\mathbf{x}\mid \mathbf{x}\in Q^n \text{ 而 } \rho(\mathbf{x}, \mathbf{c})\leqslant t\},$$

即 $S_t(\mathbf{c})$ 是由与 $\mathbf{c}$ 的距离 $\leqslant t$ 的所有的字所组成的集合. 我们把 $S_t(\mathbf{c})$ 叫做以 $\mathbf{c}$ 为中心, 以 t 为半径的球. 因 C 可以纠正 t 个差错, 所以当 $\mathbf{c}_1, \mathbf{c}_2\in C$ 而 $\mathbf{c}_1\neq\mathbf{c}_2$ 时, $S_t(\mathbf{c}_1)$ 和 $S_t(\mathbf{c}_2)$ 就没有公共元素. 如果

$$Q^n=\bigcup_{\mathbf{c}\in C}S_t(\mathbf{c}),$$

即 Q^n 分成两两没有公共元素的球 $S_t(\mathbf{c})$, $\mathbf{c}\in C$ 的并, 我们就说 C 是完全码. 换句话说, 如果任意一个字都属于一个而且唯一的一个球 $S_t(\mathbf{c})$, $\mathbf{c}\in C$, 我们就说 C 是完全码.

我们证明

定理 4 对于线性码来说, 定义 1 和定义 2 是等价的.

证. 设 C 是可以纠正 t 个差错的 q 元线性码. 先设 C 是按定义 1 来说的完全码, 即 C 的每个陪集中都有一个而且唯一的一个重量 $\leqslant t$ 的差错模式, 那么对任意一个字 $\mathbf{x}$, $\mathbf{x}$ 所属的陪集中就有唯一的一个重量 $\leqslant t$ 的差错模式 $\mathbf{e}_\lambda$. 于是 $\mathbf{x}-\mathbf{e}_\lambda\in C$. 令 $\mathbf{c}=\mathbf{x}-\mathbf{e}_\lambda$, 那么 $\mathbf{c}\in C$ 而 $\rho(\mathbf{x}, \mathbf{c})=w(\mathbf{x}-\mathbf{c})=w(\mathbf{e}_\lambda)\leqslant t$, 即 $\mathbf{x}\in S_t(\mathbf{c})$. 这就证明了 C 也是按定义 2 的意义的完全码.

反过来, 设 C 是按定义 2 的意义的完全码, 即任何一个字 $\mathbf{x}$ 都属于一个而且唯一的一个球 $S_t(\mathbf{c})$, $\mathbf{c}\in C$. 于是

$$w(\mathbf{x}-\mathbf{c})=\rho(\mathbf{x}, \mathbf{c})\leqslant t.$$

这就是说 $\mathbf{x}-\mathbf{c}$ 是一个重量 $\leqslant t$ 的差错模式, 令 $\mathbf{x}-\mathbf{c}=\mathbf{e}_\lambda$,

那么 $\mathbf{e}_\lambda$ 就是一个重量 $\leqslant t$ 的差错模式，而 $\mathbf{x}=\mathbf{e}_\lambda+\mathbf{c}\in\mathbf{e}_\lambda+C$. 这就是说 $\mathbf{x}$ 属于重量 $\leqslant t$ 的差错模式 $\mathbf{e}_\lambda$ 所属的陪集. 因此 C 也是按定义 1 的意义的完全码.

这证明了定理 4.

完全码的意义在于，收方无论收到哪一个字都可以确定把它译成那个码字，而不会发生译码不能确定的情形. 譬如，设 C 是可以纠正 t 个差错的 q 元完全码，q 是任一正整数. 当收方收到 $\mathbf{x}$ 这个字时，因 $\mathbf{x}$ 一定属于一个而且唯一的一个球 $S_t(\mathbf{c})$，$\mathbf{c}\in C$，那么 $\mathbf{x}$ 和 $\mathbf{c}$ 的距离 $\leqslant t$ 而 $\mathbf{x}$ 和其余码字的距离一定大于 t. 因此根据极大似然译码方法，就应把 $\mathbf{x}$ 译成 $\mathbf{c}$. 从前面介绍的译码表来说，完全码的译码表中没有虚线，或者说虚线下面没有字. 但这并不排斥可能发生译码错误的情况. 特别，如果一个码字在传送过程中有 $\geqslant t+1$ 个码元被传错，那就肯定发生译码错误.

从另一方面来看，设 C 是码长 n 的可以纠正 t 个差错的 q 元码，q 是任一正整数，并假定 C 含 $|C|$ 个码字. 将 $|C|$ 表作 q^k，$|C|=q^k$，即 $k=\log_q|C|$. 注意 k 不一定是整数. 定义 C 的信息率 R 为

$$R=\frac{k}{n}=\frac{1}{n}\log_q|C|,$$

那么 $|C|=q^{nR}$. 显然 $S_t(\mathbf{c})$，$\mathbf{c}\in C$，这些球两两没有公共元素，而

$$\bigcup_{\mathbf{c}\in C}S_t(\mathbf{c})\subset Q^n. \tag{7}$$

又显然 $S_t(\mathbf{c})$ 这些球都含同样个数的元素，实际上

$$|S_t(\mathbf{c})|=\sum_{j=0}^{t}\binom{n}{j}(q-1)^j.$$

因此由(7)式推出

$$q^{nR}|S_t(\mathbf{c})|\leqslant q^n,$$

即
$$|S_t(\mathbf{c})|\leqslant q^{n(1-R)},\quad \mathbf{c}\in C.$$

这就是著名的容积界. 因此，当 n 和 t 给定时，完全码是容积界中不等式取等号的码，即信息率最高的码.

显然仅由一个码字组成的码长 n 的 q 元码可以纠正 $t=n$ 个差错，而且是一个完全码；码长 $n=2t+1$ 的可以纠正 t 个差错的二元码由 (0, 0, …, 0) 和 (1, 1, …, 1) 这两个码字组成，它也是一个完全码，这两个完全码都是不足道的完全码.

此外，人们还发现可以纠正三个差错的二元 (23, 12) Golay 码和可以纠正两个差错的三元 (11, 6)Golay 码也是完全码.

最近 A. Tietäväinen* 证明，如果限定字母表是 q 个元素的有限域 $\mathbf{F}_q$，那么除了上述 Hamming 码，两个不足道的完全码和两个 Golay 码之外，不再有其他的完全码.

我们知道二元 Hamming 码的极小重量等于 3，因此二元 Hamming 码可以检查出两个差错，即码字在信道中传输时，如果有 $\leqslant 2$ 个位置的码元被传错，那么收方可以从收到的字判断出传输过程中发生差错，但是否能判断究竟错了几位呢？如果一个码，它的码字在传输过程错了 $\leqslant t$ 位时，收方从收到的字不但可以判断出传输过程中发生差错，而且可以判断出究竟错了几位，我们就说这个码是可以**确检 t 个差错的检错码**. 我们有

定理 5 二元 $(2^r-1,\ 2^r-1-r)$ Hamming 码是可以检查出两个差错的检错码，但不能确检两个差错.

证. 因二元 Hamming 码是完全码，所以任意一个重量等于 2 的差错模式的校验子必与某一个重量等于 1 的差错模

* Tietäväinen, A., On the Nonexistence of Perfect Codes over Finite Fields, SIAM Journal on Applied Mathematics, **24** (1973), 88—96.

式的校验子完全一样．因此当收方从收到的字 $\mathbf{x}$ 的校验子 $H\mathbf{x}'\neq\mathbf{0}'$ 判断出传输过程中发生差错时，却不能判断究竟错了一位还是两位．

一般地，我们有：可以纠正 t 个差错的完全码不能确检 $t+1$ 个差错．

我们可以用扩充码的方法把二元 Hamming 码扩充成一个可以确检两个差错的线性码．这是

定理 6　设 C 是二元 $(2^r-1,\ 2^r-1-r)$ Hamming 码，它的校验矩阵是 H．令

$$C_E=\left\{(c_\infty,\ c_0,\ c_1,\ \cdots,\ c_{2^r-2})\,\middle|\,(c_0,\ c_1,\ \cdots,\ c_{2^r-2})\in C\ \text{而}\ c_\infty=\sum_{i=0}^{2^r-2}c_i\right\}$$

那么 C_E 是可以确检两个差错的二元 $(2^r,\ 2^r-1-r)$ 线性码，并以

$$\begin{pmatrix} 1 & 1 \quad 1\cdots 1 \\ 0 & \\ 0 & H \\ \vdots & \\ 0 & \end{pmatrix} \tag{8}$$

为校验矩阵．

证．因 C_E 中码字的重量都是偶数，而 C 的极小重量等于 3，所以 C_E 的极小重量等于 4．因此 2 位差错的差错模式的校验子不可能等于 1 位差错的差错模式的校验子．

当然也可以先直接验证 C_E 以 (8) 为校验矩阵．然后就可以看出 2 位差错的差错模式的校验子的第一分量等于 0，而 1 位差错的差错模式的校验子的第一个分量等于 1．

§5 BCH 码

我们先回忆一下二元 Hamming 码的定义. 设 r 是个大于 1 的整数. 再设 α 是 $\mathbf{F}_{2^r}$ 的一个本原元, 那么 α^j, $j=0, 1, 2, \cdots, 2^r-2$, 就是 $\mathbf{F}_{2^r}$ 中全部不等于 0 的元素. 将它们表成 $\alpha^0=1, \alpha^1, \alpha^2, \cdots, \alpha^{r-1}$ 的线性组合

$$\alpha^j=\sum_{i=0}^{r-1} a_{ij}\alpha^i, \quad j=0, 1, 2, \cdots, 2^r-2,$$

其中 $a_{ij}\in\mathbf{F}_2$. 这样每个 $\alpha^j(0\leqslant j\leqslant 2^r-2)$ 都唯一地确定 $\mathbf{F}_2$ 上一个 r 维列向量

$$\begin{pmatrix} a_{0j} \\ a_{1j} \\ \vdots \\ a_{r-1j} \end{pmatrix},$$

这 2^r-1 个列向量两两相异. 将这 2^r-1 个列向量按 $j=0, 1, 2, \cdots, 2^r-2$ 为序排成 $\mathbf{F}_2$ 上的一个 $r\times(2^r-1)$ 矩阵

$$H=\begin{pmatrix} a_{00} & a_{01} & a_{02} & \cdots & a_{02^r-2} \\ a_{10} & a_{11} & a_{12} & \cdots & a_{12^r-2} \\ a_{20} & a_{21} & a_{22} & \cdots & a_{22^r-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{r-10} & a_{r-11} & a_{r-12} & \cdots & a_{r-12^r-2} \end{pmatrix},$$

那么 $\operatorname{rank}H=r$, 而以 H 为校验矩阵的二元 $(2^r-1, 2^r-1-r)$ 线性码就叫二元 $(2^r-1, 2^r-1-r)$ Hamming 码. 我们总是把 H 简记作

$$H=(1, \alpha, \alpha^2, \cdots, \alpha^{2^r-2}),$$

其中 α^j 代表 $\mathbf{F}_{2^r}$ 中元素 α^j 所确定的 r 维列向量 $(a_{0j}, a_{1j}, \cdots, a_{r-1j})'$, $j=0, 1, 2, \cdots, 2^r-2$. 这样一来, 容易看出二元 Hamming 码是循环码, 以 α 的极小多项式为生成多项式.

二元 Hamming 码可以很自然地作如下的推广：

设 d 是个整数，而 $1<d<n$. 我们构造 $\mathbf{F}_2$ 上的一个 $r(d-1)\times(2^r-1)$ 矩阵

$$\begin{pmatrix} 1 & \alpha, & \alpha^2, & \cdots, & \alpha^{2^r-2} \\ 1 & \alpha^2, & (\alpha^2)^2, & \cdots, & (\alpha^2)^{2^r-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{d-1}, & (\alpha^{d-1})^2, & \cdots, & (\alpha^{d-1})^{2^r-2} \end{pmatrix}, \tag{1}$$

其中 α^j 仍和上面一样代表 $\mathbf{F}_{2^r}$ 中元素 α^j 所确定的 r 维列向量 $(a_{0j}, a_{1j}, a_{2j}, \cdots, a_{rj})'$, $0\leqslant j\leqslant 2^r-2$. 我们把这个矩阵记作 H. 一般说来，H 的秩小于 $r(d-1)$. $V_{2^r-1}(\mathbf{F}_2)$ 中所有适合条件

$$H\mathbf{c}'=\mathbf{0}'$$

的向量 $\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{2^r-2})$ 组成一个子空间. 我们把这个子空间叫做设计距离 d 的二元本原 BCH 码. 象 Hamming 码一样，可以证明它是个循环码，以 α 的极小多项式 $m_1(x)$, α^2 的极小多项式 $m_2(x)$, $\cdots$ 和 α^{d-1} 的极小多项式 $m_{d-1}(x)$ 的最低公倍式

$$[m_1(x), m_2(x), \cdots, m_{d-1}(x)]$$

为生成多项式，它的码长是 2^r-1.

自然可以把二元本原 BCH 码推广成 q 元本元 BCH 码，这里 q 是一个素数的幂. 更进一步，它还可以作如下的推广.

设 q 是一个素数的幂，n 是与 q 互素的一个大于 1 的整数. 假定 q 在群 $\mathbf{Z}_n^*$ 中的阶是 r. 设 $\mathbf{F}_{q^r}$ 是 q^r 个元素的有限域，它包有 $\mathbf{F}_q$ 作为子域. 再设 α 是 $\mathbf{F}_{q^r}^*$ 中的一个 n 阶元. 实际上，如果 ξ 是 $\mathbf{F}_{q^r}$ 的一个本原元，那么 $\alpha=\xi^{(q^r-1)/n}$ 就是 $\mathbf{F}_{q^r}^*$ 中的一个 n 阶元. 因 q 在群 $\mathbf{Z}_n^*$ 中的阶是 r，所以根据第一章 §5 定理 7，α 在 $\mathbf{F}_q$ 上的极小多项式是 r 次的. 这样 $1, \alpha, \alpha^2, \cdots, \alpha^{r-1}$ 就是 $\mathbf{F}_{q^r}$ 在 $\mathbf{F}_q$ 上的一组基. 于是 α 的任意一个

幂 $\alpha^j(0\leqslant j\leqslant n-1)$ 都可以唯一地表成它们的线性组合，而系数属于 $\mathbf{F}_q$:

$$\alpha^j=\sum_{i=0}^{r-1}a_{ij}\alpha^i,\quad a_{ij}\in\mathbf{F}_q.$$

这样每个 α^j 都唯一确定 $\mathbf{F}_q$ 上的一个 r 维列向量

$$\alpha^j\to\begin{pmatrix}a_{0j}\\a_{1j}\\a_{2j}\\\vdots\\a_{r-1j}\end{pmatrix}.$$

设 d 是一个整数，而 $1<d<n$. 我们构造一个 $r(d-1)\times n$ 矩阵

$$H=\begin{pmatrix}1&\alpha&\alpha^2&\cdots&\alpha^{n-1}\\1&\alpha^2&(\alpha^2)^2&\cdots&(\alpha^2)^{n-1}\\\cdots&\cdots&\cdots&\cdots&\cdots\\1&\alpha^{d-1}&(\alpha^{d-1})^2&\cdots&(\alpha^{d-1})^{n-1}\end{pmatrix},\tag{2}$$

其中 $\alpha^j(0\leqslant j\leqslant n-1)$ 表示 $\mathbf{F}_{q^r}$ 中元素 α^j 所唯一确定的列向量 $(a_{0j},a_{1j},\cdots,a_{r-1j})'$. 一般说来 H 的秩小于 $r(d-1)$. 但 $V_n(\mathbf{F}_q)$ 中所有适合条件

$$H\mathbf{c}'=\mathbf{0}'$$

的向量 $\mathbf{c}=(c_0,c_1,c_2,\cdots,c_{n-1})$ 仍组成一个子空间. 我们把这个子空间叫做码长 n 的设计距离 d 的 q 元(非本原) BCH 码. 当 $n=q^r-1$ 时，即 α 是 $\mathbf{F}_{q^r}$ 中的本原元时，我们就得到设计距离 d 的码长 q^r-1 的 q 元本原 BCH 码.

我们先证明

定理 1 设计距离 d 的码长 n 的 q 元 BCH 码是循环码，它的生成多项式是

$$[m_1(x),m_2(x),\cdots,m_{d-1}(x)],$$

其中 $m_j(x)$ 是 $\alpha^j(1\leqslant j\leqslant d-1)$ 的极小多项式. 实际上，它的

生成多项式就是从 $m_1(x), m_2(x), \cdots, m_{d-1}(x)$ 中删去重复的以后剩下的多项式的乘积，也是 $\alpha, \alpha^2, \cdots, \alpha^{d-1}$ 都适合的次数最低的首项系数等于1的多项式.

证. 设 $\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{n-1})$是一个码字，那么 $H\mathbf{c}'=\mathbf{0}'$，即

$$c_0+c_1\alpha^j+c_1(\alpha^j)^2+\cdots+c_{n-1}(\alpha^j)^{n-1}=0,$$
$$j=1, 2, \cdots, d-1.$$

这就是说 $\alpha, \alpha^2, \cdots, \alpha^{d-1}$ 都是多项式

$$c(x)=c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}$$

的根. 因此 $m_j(x)\,|\,c(x),\quad j=1, 2, \cdots, d-1$. 令

$$m(x)=[m_1(x), m_2(x), \cdots, m_{d-1}(x)],$$

那么

$$m(x)\,|\,c(x).$$

反过来，如果 $m(x)\,|\,c(x)$，而 $c(x)=\sum_{i=0}^{n-1}c_ix^i$. $c_i\in\mathbf{F}_q$，那么 $\alpha, \alpha^2, \cdots, \alpha^{d-1}$ 都是 $c(x)$ 的根. 于是 $H\mathbf{c}'=\mathbf{0}'$，而 $\mathbf{c}=(c_0, c_1, \cdots, c_n)$. 这就是说 $\mathbf{c}$ 是一个码字.

这样定理1就完全证明了.

我们再证明

定理2 设计距离 d 的码长 n 的 q 元 BCH 码的极小距离 $\geqslant d$，因而是可以纠正$[(d-1)/2]$个差错的纠错码.

证. 用 $\mathbf{h}_0', \mathbf{h}_1', \mathbf{h}_2', \cdots, \mathbf{h}_{n-1}'$，依序代表 H 的第0列，第1列，第2列，…，第 $n-1$ 列. 如果 H 的 n 个列有一个线性关系

$$c_0\mathbf{h}_0'+c_1\mathbf{h}_1'+c_2\mathbf{h}_2'+\cdots+c_{n-1}\mathbf{h}_{n-1}'=\mathbf{0}',\quad c_i\in\mathbf{F}_q,$$

令

$$\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{n-1}),$$

那么

$$H\mathbf{c}'=\mathbf{0}'.$$

这就是说 $\mathbf{c}$ 是一个码字. 因此要证明设计距离 d 的码长 n 的 BCH 码的极小距离 $\geqslant d$，只要证明 H 的任意 $d-1$ 个列都在

$\mathbf{F}_q$ 上线性无关即可。

任选 H 的 $d-1$ 列：第 i_1 列，第 i_2 列，…，第 i_{d-1} 列，$0\leqslant i_1<i_2<\cdots<i_{d-1}\leqslant n-1$. 令 $\beta_1=\alpha^{i_1}$，$\beta_2=\alpha^{i_2}$，…，$\beta_{d-1}=\alpha^{i_{d-1}}$，那么 H 的第 i_1 列，第 i_2 列，…，第 i_{d-1} 列构成的子矩阵就是 $r(d-1)\times(d-1)$ 矩阵

$$H_{i_1i_2\cdots i_{d-1}}=\begin{pmatrix}\beta_1 & \beta_2 & \cdots & \beta_{d-1}\\ \beta_1^2 & \beta_2^2 & \cdots & \beta_{d-1}^2\\ \vdots & \vdots & & \vdots\\ \beta_1^{d-1} & \beta_2^{d-1} & \cdots & \beta_{d-1}^{d-1}\end{pmatrix}.$$

可将 $H_{i_1i_2\cdots i_{d-1}}$ 看作 $\mathbf{F}_{q^r}$ 上的一个 $(d-1)\times(d-1)$ 矩阵. 如将 $H_{i_1i_2\cdots i_{d-1}}$ 看作 $\mathbf{F}_{q^r}$ 上的 $(d-1)\times(d-1)$ 矩阵，它的列在 $\mathbf{F}_{q^r}$ 上线性无关，那么将它看作 $\mathbf{F}_q$ 上的 $r(d-1)\times d-1$ 矩阵，它的列自然在 $\mathbf{F}_q$ 上线性无关. 要证将 $H_{i_1i_2\cdots i_{d-1}}$ 看作 $\mathbf{F}_{q^r}$ 上的 $(d-1)\times(d-1)$ 矩阵时它的列在 $\mathbf{F}_{q^r}$ 上线性无关，只要证明它的秩等于 $d-1$ 就行了，而这只要证明它的行列式不等于 0 就行了. 我们有

$$|H_{i_1i_2\cdots i_{d-1}}|=\beta_1\beta_2\cdots\beta_{d-1}\begin{vmatrix}1 & 1 & \cdots & 1\\ \beta_1 & \beta_2 & \cdots & \beta_{d-1}\\ \beta_1^2 & \beta_2^2 & \cdots & \beta_{d-1}^2\\ \cdots & \cdots & \cdots & \cdots\\ \beta_1^{d-2} & \beta_2^{d-2} & \cdots & \beta_{d-1}^{d-2}\end{vmatrix},$$

上式右方的行列式是范德蒙德行列式，因 α 是 n 阶元，所以 $\beta_1=\alpha^{i_1}$，$\beta_2=\alpha^{i_2}$，…，$\beta_{d-1}=\alpha^{i_{d-1}}$ $(0\leqslant i_1<i_2<\cdots<i_{d-1}\leqslant n-1)$ 是 $d-1$ 个两两不等的非零元. 因此上式右方不等于 0. 于是

$$|H_{i_1i_2\cdots i_{d-1}}|\neq 0.$$

这证明了 H 的任意 $d-1$ 列都线性无关. 因此设计距离 d 的码长 n 的 q 元 BCH 码的极小距离 $\geqslant d$.

我们举一个例子. 考察设计距离 9 的码长 31 的二元本

原 BCH 码. 设 α 是 $\mathbf{F}_{2^5}$ 的一个本原元, 那么

$$\begin{aligned} m_1(x) &= m_2(x) = m_4(x) = m_8(x) \\ &= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16}), \\ m_3(x) &= m_6(x) \\ &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{17}), \\ m_5(x) &= (x-\alpha^5)(x-\alpha^{10})(x-\alpha^{20})(x-\alpha^9)(x-\alpha^{18}) \\ &= m_9(x) = m_{10}(x), \end{aligned}$$

因此它的极小多项式

$$g(x) = m_1(x)m_3(x)m_5(x)m_7(x)$$

以 α, α^2, $\cdots$, α^{10} 为根. 于是 $g(x)$ 就生成一个极小距离 $\geqslant 11$ 的循环码, 而定理 2 只保证 $g(x)$ 的极小距离 $\geqslant 9$. 求 BCH 码的极小距离的确切值, 是一个有意义的问题.

另一个问题是计算 BCH 码的信息位的个数, 在本书所附参考书目里[17]的第十二章有解决这个问题的一个算法. 重要的是 BCH 码的信息率比较高, 以二元本原 BCH 码为例. 即取 $q=2$ 而 $n=q^r-1$. 这时设计距离 $2t+1$ 的二元本原 BCH 码的校验矩阵可从矩阵

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{2t-1} & (\alpha^{2t-1})^2 & \cdots & (\alpha^{2t-1})^{n-1} \end{pmatrix}$$

中选线性无关行向量的一个极大组得到, 因此这个码的信息率 $\geqslant 1-\dfrac{rt}{2^r-1}$.

正是因为 BCH 码的信息率比较高, 它就受到人们很大的注意. 特别是对它的译码方法进行了很多研究, 从而发展了代数译码方法. 下面我们将介绍这个方法.

我们先作一些说明. 设 C 是个设计距离等于 $2t+1$ 的码

长等于 n 的 q 元 BCH 码，以

$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & \cdots & (\alpha^{2t})^{n-1} \end{pmatrix} \tag{3}$$

为校验矩阵，其中 α 是 $\mathbf{F}_{q^r}^*$ 中的一个 n 阶元，而 r 是 q 在群 $\mathbf{Z}_n^*$ 中的阶. 和 Hamming 码一样，我们把 $V_n(\mathbf{F}_q)$ 中的向量的诸分量从左往右依序叫做 α^0 位，α^1 位，α^2 位，$\cdots$，α^{n-1} 位的分量. 设发方发出 C 的一个码字 $\mathbf{c}$，而收方收到的是 $\mathbf{r}$，那么 $\mathbf{e}=\mathbf{r}-\mathbf{c}$ 就是码字 $\mathbf{c}$ 在信道中传送时产生的差错模式. 设 $w(\mathbf{e})=e\leqslant t$，那么 $\mathbf{e}$ 顶多有 t 个分量不等于 0. 假定 $\mathbf{e}$ 的 X_1 位，X_2 位，$\cdots$，X_e 位的分量分别是 $\mathbf{F}_q$ 中的非零元素 Y_1，Y_2，$\cdots$，Y_e，这里 X_1，X_2，$\cdots$，X_e 是 α 的 e 个两两不同的幂 α^{i_1}，α^{i_2}，$\cdots$，$\alpha^{i_e}(0\leqslant i_1, i_2, \cdots, i_e\leqslant n-1)$，而 $\mathbf{e}$ 的其余各位都等于 0，那么 $X_1, X_2, \cdots, X_e\in\mathbf{F}_{q^r}$，而 $Y_1, Y_2, \cdots, Y_e\in\mathbf{F}_q$. 我们把 $X_1, X_2, \cdots, X_e$ 叫做错位，而 $Y_1, Y_2, \cdots, Y_e$ 叫做相应这些错位的错值. 译码的任务就是要从收到的字 $\mathbf{r}$ 求出错位 $X_1, X_2, \cdots, X_e$ 和相应的错值 $Y_1, Y_2, \cdots, Y_e$，这样就求出了 $\mathbf{e}$，然后就将 $\mathbf{r}$ 译成 $\mathbf{r}-\mathbf{e}=\mathbf{c}$.

为了便于了解 BCH 码的代数译码方法，我们先举设计距离等于 5 的二元 BCH 码为例，来说明这个方法的主要步骤.

设 n 是个奇数，2 在群 $\mathbf{Z}_n^*$ 中的阶是 r，α 是 $\mathbf{F}_{2^r}$ 中的一个 n 阶元. 令

$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{n-1} \\ 1 & \alpha^4 & (\alpha^4)^2 & \cdots & (\alpha^4)^{n-1} \end{pmatrix},$$

那么 $V_n(\mathbf{F}_2)$ 中所有适合条件 $H\mathbf{c}'=\mathbf{0}'$ 的向量 $\mathbf{c}$ 就组成设计

距离5的码长n的二元BCH码. 将这个码记作C. 根据定理2, C是可以纠正两个差错的纠错码. 设在数字通信中采用C作为纠错码. 设发方发出一个码字$\mathbf{c}$, 而收方收到一个字$\mathbf{r}$, 那么$\mathbf{e}=\mathbf{r}-\mathbf{c}$就是差错模式. 假定$w(\mathbf{e})\leqslant 2$. 设$\mathbf{e}$的$X_1$位和$X_2$位的分量可能等于1, 而其余的分量都等于0.

译码的第一步是计算校验子

$$\mathbf{s}'=H\mathbf{r}'=H(\mathbf{c}+\mathbf{e})'=H\mathbf{e}'.$$

记$\mathbf{s}=(s_1, s_2, s_3, s_4)$, 我们有

$$s_j=X_1^j+X_2^j, \quad j=1, 2, 3, 4.$$

因$s_2=s_1^2$, $s_4=s_2^2=s_1^4$, 所以只要知道s_1和s_3就行了. 设$\mathbf{r}=(r_0, r_1, r_2, \cdots, r_{n-1})$, 那么

$$s_1=r_0+r_1\alpha+r_2\alpha^2+\cdots+r_{n-1}\alpha^{n-1},$$

$$s_3=r_0+r_1\alpha^3+r_2(\alpha^3)^2+\cdots+r_{n-1}(\alpha^3)^{n-1}.$$

因此s_1和s_3可以利用两个分别以α的极小多项式和以α^3的极小多项式为除式的除法电路算出.

译码的第二步是计算找错位多项式

$$\sigma(z)=(1-X_1z)(1-X_2z)$$

$$=1-(X_1+X_2)z+X_1X_2z^2.$$

(注意$\sigma(z)$的根正好是$\mathbf{c}$的错位的逆.) 分以下几个情形讨论.

1) $s_1=s_3=0$. 由

$$s_1=X_1+X_2=0, \quad s_3=X_1^3+X_2^3=0$$

推出$X_1=X_2=0$. 因此

$$\sigma(z)=1.$$

2) $s_1\neq 0$而$s_3=s_1^3$. 这时由

$$s_1^3=(X_1+X_2)^3=X_1^3+X_1X_2(X_1+X_2)+X_2^3$$

$$=s_3+X_1X_2s_1 \tag{4}$$

及$s_3=s_1^3$推出$X_1X_2s_1=0$. 因此X_1和X_2中一定有一个而

且只有一个等于0. 不妨设 $X_2=0$. 那么

$$\sigma(z)=1-X_1z.$$

3) $s_1\neq 0$, $s_3\neq s_1^3$. 这时从(4)式推出 $X_1X_2=s_1^2+\frac{s_3}{s_1}$. 因此找错位多项式是

$$\sigma(z)=1+s_1z+\left(s_1^2+\frac{s_3}{s_1}\right)z^2.$$

译码的第三步是求找错位多项式 $\sigma(z)$ 的根，然后改正 $\mathbf{c}$ 在传送过程中出现的差错. 仍分上面三个情形讨论.

1) $s_1=s_3=0$. 这时 $\sigma(z)=1$. 这说明 $\mathbf{c}$ 在传送过程中没有出现差错. 因此 $\mathbf{r}=\mathbf{c}$.

2) $s_1\neq 0$ 而 $s_3=s_1^3$. 这时 $\sigma(z)=1-X_1z$. 这说明 $\mathbf{c}$ 在传送过程中出现了一个差错. 设 $X_1=\alpha^{-i}(0\leqslant i\leqslant n-1)$. 这表明 $\mathbf{c}$ 在传送过程中仅 α^i 位发生差错. 这时将 $\mathbf{r}$ 的 α^i 位的值加以改变(即如果 $\mathbf{r}$ 的 α^i 位的值是 0, 就改成 1, 而如果是 1, 就改成 0), 就得到 $\mathbf{c}$.

3) $s_1\neq 0$ 而 $s_3\neq s_1^3$. 这时 $\sigma(z)$ 是个二次多项式，用试探法求这个多项式的根，即将 $\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{n-1}$ 逐个地代入 $\sigma(z)$ 看是否得0. 设 $\sigma(z)$ 的两个根是 $\alpha^{-i}, \alpha^{-j}(0\leqslant i<j\leqslant n-1)$, 这表明 $\mathbf{c}$ 在传送过程中 α^i 位和 α^j 位的码元被传错. 这时将 $\mathbf{r}$ 的 α^i 位和 α^j 位的值加以改变，就得到 $\mathbf{c}$.

现在我们来介绍设计距离等于 $2t+1$ 而码长等于 n 的 q 元 BCH 码的代数译码方法. 用 C 代表这个码，它的校验矩阵是(3)中的 H. 我们知道 C 是可以纠正 t 个差错的纠错码. 设在数字通信中选用了 C 作为纠错码. 设码字 $\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{n-1})$ 被传送，即发方发出码字 $\mathbf{c}$, 再设收方收到的字是 $\mathbf{r}=(r_0, r_1, r_2, \cdots, r_{n-1})$. 那么差错模式是

$$\mathbf{e}=\mathbf{r}-\mathbf{c}=(e_0, e_1, e_2, \cdots, e_{n-1}).$$

收方译码器的任务就是如何从 $\mathbf{r}$ 求出 $\mathbf{e}$, 从而正确译出 $\mathbf{c}=$

$\mathbf{r}-\mathbf{e}$. 译码分四步进行:

译码的第一步是计算校验子,即计算

$$\mathbf{s}'=H\mathbf{r}',$$

其中 $\mathbf{s}=(s_1, s_2, \cdots, s_{2t})$, 而

$$s_i=r_0+r_1\alpha^i+r_2(\alpha^i)^2+\cdots+r_{n-1}(\alpha^i)^{n-1},$$

$$i=1, 2, \cdots, 2t.$$

我们知道, s_i 的计算可以利用以 α^i 的极小多项式作除式的除法电路来实现.

设 $w(\mathbf{e})=e\leqslant t$, 并设 $\mathbf{e}$ 的 X_1 位, X_2 位, $\cdots$, X_e 位的分量分别是 $\mathbf{F}_q$ 中的非零元素 $Y_1, Y_2, \cdots, Y_e$, 而 $\mathbf{e}$ 的其余位置的分量都等于 0. 我们有 $X_j\in\mathbf{F}_{q^r}$ 而 $Y_j\in\mathbf{F}_q(j=1,2,\cdots,e)$. 译码器的任务就是要从第一步算出的校验子 $\mathbf{s}'=H\mathbf{r}'$, 算出错位 $X_1, X_2, \cdots, X_e$ 和相应的错值 $Y_1, Y_2, \cdots, Y_e$, 这样就求出了 $\mathbf{e}$, 然后就可以把 $\mathbf{r}$ 正确译成 $\mathbf{r}-\mathbf{e}=\mathbf{c}$.

译码的第二步是从第一步算出的校验子 $\mathbf{s}'=H\mathbf{r}'$ 算出找错位多项式

$$\sigma(z)=(1-X_1z)(1-X_2z)\cdots(1-X_ez).$$

令
$$\sigma(z)=1+\sigma_1z+\sigma_2z^2+\cdots+\sigma_ez^e,$$

而 $\mathbf{s}=(s_1, s_2, \cdots, s_{2t})$, 那么这就是说要从 $s_1, s_2, \cdots, s_{2t}$ 算出 $\sigma_1, \sigma_2, \cdots, \sigma_e$. 因为一般说来 $e>2$, 这时问题就比前面举的例子复杂了.

令
$$c(x)=c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1},$$
$$r(x)=r_0+r_1x+r_2x^2+\cdots+r_{n-1}x^{n-1},$$
$$e(x)=e_0+e_1x+e_2x^2+\cdots+e_{n-1}x^{n-1},$$

那么 $c(x)=r(x)-e(x)$. 显然有 $c(\alpha^i)=0$, 因此

$$s_i=r(\alpha^i)=e(\alpha^i), \quad i=1, 2, \cdots, 2t. \tag{5}$$

可以将(5)写成

$$s_i=\sum_{j=1}^{e} Y_j X_j^i, \quad i=1, 2, \cdots, 2t. \tag{6}$$

将 $(1-X_jz)^{-1}$ 表成

$$\frac{1}{1-X_jz}=1+X_jz+X_j^2z^2+\cdots+X_j^{2t-1}z^{2t-1}+\frac{X_j^{2t}z^{2t}}{1-X_jz}.$$

将上式双方乘以 Y_jX_j, 然后再对 j 求和, 利用(6)式可得

$$\sum_{j=1}^{e}\frac{Y_jX_j}{1-X_jz}=s(z)+\sum_{j=1}^{e}\frac{Y_jX_j^{2t+1}z^{2t}}{1-X_jz}, \tag{7}$$

其中置 $\qquad s(z)=s_1+s_2z+s_3z^2+\cdots+s_{2t}z^{2t-1}.$

再令 $\qquad \omega(z)=\sum_{j=1}^{e}Y_jX_j\prod_{\substack{k=1\\k\neq j}}^{e}(1-X_kz),$

那么

$$\frac{\omega(z)}{\sigma(z)}=\sum_{j=1}^{e}\frac{Y_jX_j}{1-X_jz}. \tag{8}$$

由(7), (8)两式推出

$$\frac{\omega(z)}{\sigma(z)}=s(z)+\sum_{j=1}^{e}\frac{Y_jX_j^{2t+1}z^{2t}}{1-X_jz}.$$

于是

$$\omega(z)=s(z)\sigma(z)+\varphi(z), \tag{9}$$

其中

$$\begin{aligned}\varphi(z)&=\sum_{j=1}^{e}\frac{Y_jX_j^{2t+1}z^{2t}}{1-X_jz}\sigma(z)\\&=\sum_{j=1}^{e}Y_jX_j^{2t+1}z^{2t}\prod_{\substack{k=1\\k\neq j}}^{e}(1-X_kz).\end{aligned}$$

注意 $\varphi(z)$ 是一个多项式, 它的 i 次项$(0\leqslant i\leqslant 2t-1)$的系数都等于0, 那么由(9)式推出

$$\omega(z)\equiv s(z)\sigma(z) \pmod{z^{2t}}. \tag{10}$$

注意有 $\qquad \sigma(0)=1,$

$$\partial^0\sigma(z)=e, \quad \partial^0\omega(z)<e,$$

而且容易证明

$$(\sigma(z), \omega(z))=1.$$

写

$$\sigma(z)=1+\sigma_1 z+\sigma_2 z^2+\cdots+\sigma_e z^e,\quad \sigma_e\neq 0,\ \sigma_i\in\mathbf{F}_{q^r},$$

$$\omega(z)=\omega_0+\omega_1 z+\omega_2 z^2+\cdots+\omega_{e-1}z^{e-1},\quad \omega_i\in\mathbf{F}_{q^r},$$

那么比较(10)式双方零次项，一次项，…，直到 $2t-1$ 次项的系数，得出下面的关系式

$$\begin{pmatrix}\omega_0\\ \omega_1\\ \omega_2\\ \vdots\\ \omega_{e-1}\end{pmatrix}=\begin{pmatrix}1 & & & \\ \sigma_1 & 1 & & 0\\ \sigma_2 & \sigma_1 & 1 & \\ \vdots & \ddots & \ddots & \ddots\\ \sigma_{e-1}\cdots\sigma_2 & & \sigma_1 & 1\end{pmatrix}\begin{pmatrix}s_1\\ s_2\\ s_3\\ \vdots\\ s_e\end{pmatrix},$$

以及

$$s_k+\sigma_1 s_{k-1}+\sigma_2 s_{k-2}+\cdots+\sigma_e s_{k-e}=0,$$

$$k=e+1,\ e+2,\ \cdots,\ 2t. \tag{11}$$

这就是说 $\sigma_1,\sigma_2,\cdots,\sigma_e$ 必需适合(11)式．换句话说，$\langle\sigma(z),e\rangle$ 就是产生长为 $2t$ 的 q^r 元序列

$$s_1,\ s_2,\ \cdots,\ s_{2t} \tag{12}$$

的一个线性移位寄存器．

我们先证明

引理 1 假定 $e\leqslant t$．如果$\langle\hat{\sigma}(z),\hat{e}\rangle$是产生(12)的一个最短线性移位寄存器，那么一定有

$$\hat{\sigma}(z)=\sigma(z),\quad \hat{e}=e.$$

证．设 $\langle\hat{\sigma}(z),\hat{e}\rangle$ 是产生(12)的一个最短线性移位寄存器，那么 $\hat{e}\leqslant e$．令

$$\hat{\sigma}(z)=1+\hat{\sigma}_1 z+\hat{\sigma}_2 z^2+\cdots+\hat{\sigma}_{\hat{e}}z^{\hat{e}},$$

那么

$$s_k+\hat{\sigma}_1 s_{k-1}+\hat{\sigma}_2 s_{k-2}+\cdots+\hat{\sigma}_{\hat{e}}s_{k-\hat{e}}=0,$$

$$k=\hat{e}+1,\ \hat{e}+2,\ \cdots,\ 2t.$$

令

$$\hat{\omega}(z)=(s(z)\hat{\sigma}(z))_{z^{2t}}, \tag{13}$$

即 $\hat{\omega}(z)$ 是用 z^{2t} 去除 $s(z)\hat{\sigma}(z)$ 所得的余式，那么 $\partial^0\hat{\omega}(z)<\hat{e}$.

把(13)式写作

$$\hat{\omega}(z) \equiv s(z)\hat{\sigma}(z) \pmod{z^{2t}} \tag{14}$$

将(10)式双方都乘以 $\hat{\sigma}(z)$，而把(14)双方都乘以 $\sigma(z)$，所得到的两个同余式的右方相同，因此它们的左方必同余 $\bmod z^{2t}$，即

$$\hat{\sigma}(z)\omega(z) \equiv \sigma(z)\hat{\omega}(z) \pmod{z^{2t}}. \tag{15}$$

因 $\partial^0\sigma(z)=e,\ \partial^0\omega(z)<e,\ \partial^0\hat{\sigma}(z)\leqslant\hat{e},\ \partial^0\hat{\omega}(z)<\hat{e},$

而 $e\leqslant t,\quad \hat{e}\leqslant e,$

所以(15)式实际上是恒等式，即

$$\hat{\sigma}(z)\omega(z)=\sigma(z)\hat{\omega}(z).$$

但 $(\sigma(z),\ \omega(z))=1$，所以一定有

$$\sigma(z)\mid\hat{\sigma}(z).$$

可是 $\partial^0\sigma(z)=e\geqslant\hat{e}\geqslant\partial^0\hat{\sigma}(z)$，所以

$$\sigma(z)=\hat{\sigma}(z),$$

$$e=\hat{e}.$$

这证明了引理1.

根据引理1，在 $e\leqslant t$ 的前提下，$\langle\sigma(z),\ e\rangle$ 就是产生(12)的最短线性移位寄存器. 自然可以用第三章§8中所介绍的线性移位寄存器的综合算法去求产生(12)的最短线性移位寄存器. 我们把这个算法重新写在下面:

求找错位多项式的迭代算法 设收到的字 $\mathbf{r}$ 的校验子

$$s_1,\ s_2,\ \cdots,\ s_{2t}$$

已算出，对 n 用归纳法来定义一系列的线性移位寄存器

$$\langle\sigma_n(z),\ l_n\rangle,\quad n=1,\ 2,\ \cdots,\ 2t.$$

(1) 设 n_0 是个正整数使

$$s_1=s_2=\cdots=s_{n_0-1}=0,\quad s_{n_0}\neq 0,$$

那么约定 $d_0=d_1=d_2=\cdots=d_{n_0-2}=0,\quad d_{n_0-1}=s_{n_0},$

并令 $\sigma_1(z)=\sigma_2(z)=\cdots=\sigma_{n_0-1}(z)=1,$

$$l_1=l_2=\cdots=l_{n_0-1}=0;$$

$$\sigma_{n_0}(z)=1-d_{n_0-1}z^{n_0},\quad l_{n_0}=n_0.$$

(2) 设 $\langle\sigma_i(z),\ l_i\rangle$, $i=1,\ 2,\ \cdots,\ n(n_0\leqslant n<2t)$ 已求得，而

$$l_1=l_2=\cdots=l_{n_0-1}=0<l_{n_0}\leqslant l_{n_0+1}\leqslant\cdots\leqslant l_n.$$

令
$$\sigma_n(z)=1+\sigma_{n1}z+\sigma_{n2}z^2+\cdots+\sigma_{nl_n}z^{l_n}.$$

计算
$$d_n=s_{n+1}+\sigma_{n1}s_n+\sigma_{n2}s_{n-1}+\cdots+\sigma_{nl_n}s_{n-l_n+1}.$$

区别下面两个情形:

2.1) $d_n=0$. 这时令

$$\sigma_{n+1}(z)=\sigma_n(z),\quad l_{n+1}=l_n.$$

2.2) $d_n\neq0$. 这时有 $m(1\leqslant m<n)$ 使

$$l_m<l_{m+1}\leqslant l_{m+2}=\cdots=l_n.$$

那么令
$$\sigma_{n+1}(z)=\sigma_n(z)-d_nd_m^{-1}z^{n-m}\sigma_m(z),$$

$$l_{n+1}=\max\{l_n,\ n+1-l_n\}.$$

最后我们得到 $\langle\sigma_{2t}(z),\ l_{2t}\rangle$. 如果 **r** 的错位个数 $e\leqslant t$, 那么 $\sigma_{2t}(z)$ 就是找错位多项式 $\sigma(z)$，即

$$\sigma(z)=\sigma_{2t}(z).$$

当然也可以采用修饰的综合算法，这样可以使求逆元素的运算减成一次.

译码的第三步是去求错位,即求 $\sigma(z)$ 的根的逆. 我们知道，$\alpha^i(0\leqslant i\leqslant n-1)$ 是一个错位，当且仅当 $\sigma(\alpha^{-i})=0$. 这一步可以采用试探法.

设码字 $\mathbf{c}=(c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1})$ 是从足码最大的位发送起的，即先发送 c_{n-1}，再发送 c_{n-2}，…，最后发送 c_0. 采用§3中所介绍的循环码的第一种编码方法就是这样的. 这时顶好先检查 α^{n-1} 看它是不是错位，这只要检查 α 是不是 $\sigma(z)$ 的根，即

$$1+\sigma_1\alpha+\sigma_2\alpha^2+\cdots+\sigma_e\alpha^e$$

是不是等于0．因此要试探α^{n-1}是不是错位，译码器只要先算出$\sigma_1\alpha$, $\sigma_2\alpha^2$, $\cdots$, $\sigma_e\alpha^e$，然后将它们相加；如果相加的结果等于-1, α^{n-1}就是一个错位，否则就不是.

下一步是检查α^{n-2}是不是错位，和上面的道理一样，α^{n-2}是一个错位，当且仅当$\sigma(\alpha^2)=0$，因而当且仅当

$$1+\sigma_1\alpha^2+\sigma_2\alpha^{2\cdot 2}+\cdots+\sigma_e\alpha^{2e}=0.$$

因此这时译码器要先算出$\sigma_1\alpha^2$, $\sigma_2\alpha^{2\cdot 2}$, $\cdots$, $\sigma_e\alpha^{2e}$，然后将它们相加；如果结果等于-1, α^{n-2}就是一个错位；否则就不是.

一般地，$\alpha^{n-j}(j=1, 2, \cdots, n)$是一个错位，当且仅当$\sigma(\alpha^j)=0$，因而当且仅当

$$1+\sigma_1\alpha^j+\sigma_2\alpha^{j\cdot 2}+\cdots+\sigma_e\alpha^{j\cdot e}=0.$$

因此这时译码器要先算出$\sigma_1\alpha^j$, $\sigma_2\alpha^{j\cdot 2}$, $\cdots$, $\sigma_e\alpha^{j\cdot e}$，然后将它们相加；如果结果等于$-1$, α^{n-j}就是一个错位；否则就不是.

译码的第四步是计算错值．对于二元码，错值都等于1，因此这一步是不需要的．但是对于q元码，错值是$\mathbf{F}_q$中的非零元，因此这一步是需要的．我们回忆，在第二步中已经引进了

$$\omega(z)=\sum_{j=1}^{e} Y_j X_j \prod_{\substack{k=1\\k\neq j}}^{e}(1-X_k z).$$

再令
$$\sigma^{(i)}(z)=\prod_{j\neq i}(1-X_j z),\quad i=1, 2, \cdots, e.$$

将$z=X_i^{-1}$代入$\omega(z)$就得到

$$\omega(X_i^{-1})=Y_i X_i \sigma^{(i)}(X_i^{-1}).$$

因此

$$Y_i=\frac{\omega(X_i^{-1})}{X_i\sigma^{(i)}(X_i^{-1})}. \tag{16}$$

用$\hat{\omega}(z)$表与$\omega(z)$互反的多项式，并用$\tilde{\sigma}^{(i)}(z)$表与$\sigma^{(i)}(z)$互反的多项式。那么将(16)式右方分子和分母都乘以X_i^{e-1}，就有

$$Y_i=\frac{X_i^{e-1-\partial^0\omega(z)}\tilde{\omega}(X_i)}{X_i\tilde{\sigma}^{(i)}(X_i)}. \tag{17}$$

在第二步中已经证明了

$$\omega(z)\equiv s(z)\sigma(z)\quad(\operatorname{mod} z^{2t})$$

$$\partial^0\omega(z)\leqslant e-1.$$

因此 $\omega(z)$ 可以按下式算出

$$\omega(z)=(s(z)\sigma(z))_{z^e},$$

而 $\sigma^{(i)}(z)$ 可以按下式算出

$$\sigma^{(i)}(z)=\frac{\sigma(z)}{1-X_iz},$$

所以错值 Y_i 可以按公式(17)算出.

译码的最后一步就是按照所求出的错位和错值去改正收到的字里的差错. 一旦差错改正，这个字的译码工作就完成了.

应该指出，这个译码算法是可以用硬件来实现的.

对于二元 BCH 码，上述译码算法中，除了第四步不需要之外，第二步也可以化简. 我们先证明

引理 2 对于设计距离等于 $2t+1$ 而码长 n 的 q 元 BCH 码，当按照上述译码算法中第二步的迭代算法求 $\sigma(z)$ 时，令

$$\omega_n(z)=(s(z)\sigma_n(z))_{z^n},\quad n=0,\ 1,\ 2,\ \cdots,\ 2t,$$

那么当被传送的码字在信道中出现的差错个数 $e\leqslant t$ 时，一定有

1) $\partial^0\omega_n(z)<l_n.$

2) $s(z)\sigma_n(z)\equiv\omega_n(z)+d_nz^n(\operatorname{mod} z^{n+1}).$

证. 写

$$\sigma_n(z)=1+\sigma_{n1}z+\sigma_{n2}z^2+\cdots+\sigma_{nl_n}z^{l_n}.$$

因为 $\qquad l_n\leqslant n,$

$$l_n\leqslant l_{2t}=e\leqslant t,\quad n=0,\ 1,\ 2,\ \cdots,\ 2t,$$

所以

$$
\begin{aligned}
s(z)\sigma_n(z) \equiv & s_1+(s_2+\sigma_{n1}s_1)z+(s_3+\sigma_{n1}s_2+\sigma_{n2}s_1)z^2+\cdots \\
& +(s_{l_n}+\sigma_{n1}s_{l_n-1}+\sigma_{n2}s_{l_n-2}+\cdots+\sigma_{nl_n-1}s_1)z^{l_n-1} \\
& +\sum_{k=l_{n+1}}^{n}(s_k+\sigma_{n1}s_{k-1}+\sigma_{n2}s_{k-2}+\cdots \\
& +\sigma_{nl_n}s_{k-l_n})z^{k-1} \pmod{z^n}
\end{aligned}
$$

但 $\langle\sigma_n(z),\ l_n\rangle$ 是产生

$$s_1,\ s_2,\ \cdots,\ s_n$$

的一个最短线性移位寄存器，所以

$$s_k+\sigma_{n1}s_{k-1}+\sigma_{n2}s_{k-2}+\cdots+\sigma_{nl_n}s_{k-l_n}=0,$$
$$k=l_n+1,\ l_n+2,\ \cdots,\ n.$$

因此

$$
\begin{aligned}
\omega_n(z)=(s(z)\sigma_n(z))_{z^n}= & s_1+(s_2+\sigma_{n1}s_1)z \\
& +(s_3+\sigma_{n1}s_2+\sigma_{n2}s_1)z^2+\cdots \\
& +(s_{l_n}+\sigma_{n1}s_{l_n-1}+\sigma_{n2}s_{l_n-2}+\cdots+\sigma_{nl_n-1}s_1)z^{l_n-1}.
\end{aligned}
$$

于是 $$\partial^0\omega_n(z)<l_n.$$

更进一步，我们有

$$
\begin{aligned}
s(z)\sigma_n(z)\equiv & \omega_n(z)+(s_{n+1}+\sigma_{n1}s_n+\sigma_{n2}s_{n-1}+\cdots \\
& +\sigma_{nl_n}s_{n-l_n+1})z^n \pmod{z^{n+1}}.
\end{aligned}
$$

可是 $$d_n=s_{n+1}+\sigma_{n1}s_n+\sigma_{n2}s_{n-1}+\cdots+\sigma_{nl_n}s_{n-l_n+1}.$$

所以 $$s(z)\sigma_n(z)\equiv\omega_n(z)+d_nz^n \pmod{z^{n+1}}.$$

从现在起假定 $q=2$，即局限于讨论二元 BCH 码．我们要证明，在求找错位多项式 $\sigma(z)$ 的迭代算法（以下简称迭代算法）中，当 n 是奇数时 $(0<n<2t)$，总有 $d_n=0$．为了证明这一事实，我们先引进一些记号．

设 $f(z)$ 是 $\mathbf{F}_{2^r}$ 上的一个多项式．如果 $f(z)$ 中 z 的奇次方项的系数都等于 0，$f(z)$ 就叫偶多项式；如果 $f(z)$ 中 z 的偶次方项的系数都等于 0，$f(z)$ 就叫奇多项式．设

$$f(z)=a_0+a_1z+a_2z^2+a_3z^3+\cdots+a_nz^n,$$

令 $$\hat{f}(z)=a_1z+a_3z^3+a_5z^5+\cdots,$$
$$\hat{\hat{f}}(z)=a_0+a_2z^2+a_4z^4+\cdots,$$
那么 $$f(z)=\hat{f}(z)+\hat{\hat{f}}(z),$$
而$\hat{f}(z)$和$\hat{\hat{f}}(z)$分别是奇多项式和偶多项式，分别叫做$f(z)$的奇次部分和偶次部分.

假定在数字通信中采用的是一个设计距离 $2t+1$ 的码长 n 的二元 BCH 码，它的校验矩阵是(4)中的 H，而其中 α 是 $\mathbf{F}_{2^r}^*$ 中的一个 n 阶元，2 在 $\mathbf{Z}_n^*$ 中的阶是 r. 设发方发出一个码字 $\mathbf{c}$，而收方收到的字是 $\mathbf{r}$. 那么 $\mathbf{e}=\mathbf{r}-\mathbf{c}$ 就是差错模式. 和前面一样仍设 $w(\mathbf{e})=e\leqslant t$，而 $X_1, X_2, \cdots, X_e$ 是错位，即 $\mathbf{e}$ 的非零分量所在的位置. 我们有
$$s_i=\sum_{j=1}^{e}X_j^i,\quad i=1,\ 2,\ \cdots,$$
而 $$s(z)=s_1+s_2z+s_3z^2+\cdots+s_{2t}z^{2t-1}.$$
再令 $$s_0(z)=zs(z)=s_1z+s_2z^2+s_3z^3+\cdots+s_{2t}z^{2t},$$
那么我们有

引理 3 $s_0(z)^2=\hat{\hat{s}}_0(z)\pmod{z^{2t+1}}$.

证. 对任意正整数 i，我们有
$$s_i^2=\left(\sum_{j=1}^{e}X_j^i\right)^2=\sum_{j=1}^{e}X_j^{2i}=s_{2i}.\qquad(18)$$
因此
$$\begin{aligned}s_0(z)^2&=s_1^2z^2+s_2^2z^4+s_3^2z^6+\cdots+s_{2t}^2z^{4t}\\&\equiv s_2z^2+s_4z^4+s_6z^6+\cdots+s_{2t}z^{2t}\pmod{z^{2t+1}}\end{aligned}$$
但 $$\hat{\hat{s}}_0(z)=s_2z^2+s_4z^4+s_6z^6+\cdots+s_{2t}z^{2t},$$
所以 $$\hat{\hat{s}}_0(z)^2\equiv\hat{\hat{s}}_0(z)\pmod{z^{2t+1}}.$$

现在我们去证明

定理 3 对于设计距离等于 $2t+1$ 的码长等于 n 的二元 BCH 码来说，如果被传送的码字在传送过程中产生的差错个数 $e\leqslant t$，那么按照求找错位多项式 $\sigma(z)$ 的迭代算法去求 $\sigma(z)$

时，一定有

1) $z\omega_n(z)=\hat{\sigma}_n(z)$, $n=0, 1, 2, \cdots, 2t$.

2) $d_n=0$ 对于奇数 n, 即对于 $n=1, 3, 5, \cdots, 2t-1$.

证. 我们对 n 用数学归纳法来证明这个定理.

设 n_0 是个正整数使

$$s_1=s_2=\cdots=s_{n_0-1}=0, \quad s_{n_0}\neq 0.$$

那么从(18)式推出 n_0 一定是奇数. 令

$$n_0=2k_0+1.$$

根据迭代算法

$$d_0=d_1=d_2=\cdots=d_{2k_0-1}=0.$$

特别

$$d_1=d_3=\cdots=d_{2k_0-1}=0.$$

这证明了 2)对于 $n\leqslant 2k_0$ 成立.

仍根据迭代算法

$$\sigma_1(z)=\sigma_2(z)=\cdots=\sigma_{2k_0}(z)=1.$$

因此对于 $n\leqslant 2k_0$,

$$\omega_n(z)=(s(z)\sigma_n(z))_{z^{n+1}}=(s(z))_{z^{n+1}}=0.$$

于是

$$z\omega_n(z)=0.$$

显然对于 $n\leqslant 2k_0$ 有

$$\hat{\sigma}_n(z)=0.$$

因此对于 $n\leqslant 2k_0$,

$$z\omega_n(z)=\hat{\sigma}_n(z).$$

这证明了 1)对于 $n\leqslant 2k_0$ 也成立. 因此定理 3 对于 $n\leqslant 2k_0$ 成立.

现在假定定理 3 对于 n 成立, 而 $2k_0\leqslant n<2t$. 我们去证明它对于 $n+1$ 也成立，分别考察 n 是偶数和奇数这两个情形.

(1) $n=2k$ 是偶数. 先去证明 1)对于 $2k+1$ 成立. 再区别 $d_{2k}=0$ 和 $d_{2k}\neq 0$ 这两个情形.

1.1) $d_{2k}=0$. 这时根据综合算法,

$$\sigma_{2k+1}(z)=\sigma_{2k}(z), \quad l_{2k+1}=l_{2k}.$$

根据引理 2,

$$s(z)\sigma_{2k}(z)\equiv\omega_{2k}(z)+d_{2k}z^{2k}(\mathrm{mod}\ z^{2k+1})$$
$$\equiv\omega_{2k}(z)(\mathrm{mod}\ z^{2k+1}).$$

因此

$$\omega_{2k+1}(z)=(s(z)\sigma_{2k+1}(z))_{z^{2k+1}}=(s(z)\sigma_{2k}(z))_{z^{2k+1}}=\omega_{2k}(z).$$

根据归纳法假设

$$z\omega_{2k}(z)=\hat{\sigma}_{2k}(z),$$

所以
$$z\omega_{2k+1}(z)=\hat{\sigma}_{2k+1}(z).$$

1.2) $d_{2k}\neq 0$. 先考察 $k=k_0$, 即 $n=n_0-1$ 的情形, 这时根据迭代算法,

$$d_{2k_0}=s_{2k_0+1}\neq 0,$$
$$\sigma_{2k_0+1}(z)=1+d_{2k_0}z^{2k_0+1}, \quad l_{2k_0+1}=2k_0+1.$$

于是
$$\omega_{2k_0+1}(z)=(s(z)\sigma_{2k_0+1}(z))_{z^{2k_0+1}}=s_{2k_0+1}z^{2k_0},$$
$$z\omega_{2k_0+1}(z)=s_{2k_0+1}z^{2k_0+1}=\hat{\sigma}_{2k_0+1}(z).$$

再考察 $k>k_0$, 即 $n>n_0$ 的情形. 根据 n_0 的选取, 归纳法假设和迭代算法

$$d_0=d_1=d_2=\cdots=d_{2k_0-1}=0, \quad d_{2k_0}\neq 0,$$
$$d_{2k_0+1}=d_{2k_0+3}=\cdots=d_{2k-1}=0,$$
$$l_1=l_2=\cdots=l_{2k_0}=0, \quad l_{2k_0+1}=2k_0+1>0,$$
$$l_{2k_0+1}=l_{2k_0+2}\leqslant l_{2k_0+3}=l_{2k_0+4}\leqslant\cdots\leqslant l_{2k-1}=l_{2k},$$

那么有 $m(0\leqslant m<k)$ 使

$$l_{2m}<l_{2m+1}=l_{2m+2}=\cdots=l_{2k}.$$

这时
$$\sigma_{2k+1}(z)=\sigma_{2k}(z)+d_{2k}d_{2m}^{-1}z^{2(k-m)}\sigma_{2m}(z),$$
$$\omega_{2k+1}(z)=(s(z)\sigma_{2k+1}(z))_{z^{2k+1}}$$
$$=(s(z)\sigma_{2k}(z))_{z^{2k+1}}+(d_{2k}d_{2m}^{-1}z^{2(k-m)}s(z)\sigma_{2m}(z))_{z^{2k+1}}.$$

根据引理 2,

$$s(z)\sigma_{2k}(z)\equiv\omega_{2k}(z)+d_{2k}z^{2k}(\bmod z^{2k+1}),$$
$$s(z)\sigma_{2m}(z)\equiv\omega_{2m}(z)+d_{2m}z^{2m}(\bmod z^{2m+1}).$$

因此 $\qquad \omega_{2k+1}(z)=\omega_{2k}(z)+d_{2k}d_{2m}^{-1}z^{2(k-m)}\omega_{2m}(z).$

根据归纳法假设

$$z\omega_{2k}(z)=\hat{\sigma}_{2k}(z),$$
$$z\omega_{2m}(z)=\hat{\sigma}_{2m}(z).$$

所以 $\quad z\omega_{2k+1}(z)=\hat{\sigma}_{2k}(z)+d_{2k}d_{2m}^{-1}z^{2(k-m)}\hat{\sigma}_{2m}(z)=\hat{\hat{\sigma}}_{2k+1}(z).$

这证明了 1)对于 $2k+1$ 成立.

再去证明 2)对于 $2k+1$ 也成立. 根据引理 2,

$$s(z)\sigma_{2k+1}(z)\equiv\omega_{2k+1}(z)+d_{2k+1}z^{2k+1}(\bmod z^{2k+2}).$$

于是 $\quad zs(z)\sigma_{2k+1}(z)\equiv z\omega_{2k+1}(z)+d_{2k+1}z^{2k+2}(\bmod z^{2k+3}).$

刚才已经证明

$$z\omega_{2k+1}(z)=\hat{\sigma}_{2k+1}(z),$$

又根据定义 $\qquad zs(z)=s_0(z),$

所以 $\quad s_0(z)\sigma_{2k+1}(z)\equiv\hat{\hat{\sigma}}_{2k+1}(z)+d_{2k+1}z^{2k+2}(\bmod z^{2k+3}).$

比较上式双方奇次部分和偶次部分得

$$\hat{s}_0(z)\hat{\sigma}_{2k+1}(z)+(\hat{\hat{s}}_0(z)+1)\hat{\hat{\sigma}}_{2k+1}(z)\equiv 0(\bmod z^{2k+3}), \tag{19}$$
$$\hat{\hat{s}}_0(z)\hat{\sigma}_{2k+1}(z)+\hat{s}_0(z)\hat{\sigma}_{2k+1}(z)\equiv d_{2k+1}z^{2k+2}(\bmod z^{2k+3}). \tag{20}$$

将(19)式乘以 $\hat{s}_0(z)$, 将(20)式乘以 $\hat{\hat{s}}_0(z)+1$, 然后相加, 得

$$\begin{aligned}&(\hat{s}_0(z)^2+\hat{\hat{s}}_0(z)^2+\hat{\hat{s}}_0(z))\hat{\hat{\sigma}}_{2k+1}(z)\\&\equiv d_{2k+1}z^{2k+2}(\hat{\hat{s}}_0(z)+1)(\bmod z^{2k+3}).\end{aligned} \tag{21}$$

但 $\qquad \hat{s}_0(z)^2+\hat{\hat{s}}_0(z)^2=(\hat{s}_0+\hat{\hat{s}}_0(z))^2=(s(z))^2,$

而根据引理 3

$$(s(z))^2\equiv\hat{\hat{s}}_0(z)(\bmod z^{2t+1}).$$

因 $2k+1<2t$, 所以 $2k+3\leqslant 2t+1$. 因此

$$\hat{s}_0(z)^2+\hat{\hat{s}}_0(z)^2\equiv\hat{\hat{s}}_0(z)(\bmod z^{2k+3}). \tag{22}$$

将(22)式代入(21)式得

$$0\equiv d_{2k+1}z^{2k+2}(\hat{\hat{s}}_0(z)+1)(\bmod z^{2k+3}).$$

因此立刻推出 $d_{2k+1}=0$. 这证明了 2)对于 $2k+1$ 也成立.

(2) $n=2k+1$ 是奇数. 根据归纳法假设

$$z\omega_{2k+1}(z)=\hat{\sigma}_{2k+1}(z),$$

$$d_{2k+1}=0.$$

因此
$$\sigma_{2k+2}(z)=\sigma_{2k+1}(z),$$

$$\omega_{2k+2}(z)=(s(z)\sigma_{2k+2}(z))_{z^{2k+2}}=(s(z)\sigma_{2k+1}(z))_{z^{2k+2}}.$$

根据引理 2

$$s(z)\sigma_{2k+1}(z)\equiv\omega_{2k+1}(z)+d_{2k+1}z^{2k+1}(\bmod z^{2k+2}).$$

因 $d_{2k+1}=0$, 所以

$$\omega_{2k+1}(z)=(s(z)\sigma_{2k+1}(z))_{z^{2k+2}}.$$

因此
$$\omega_{2k+2}(z)=\omega_{2k+1}(z).$$

于是
$$z\omega_{2k+2}(z)=z\omega_{2k+1}(z)=\hat{\sigma}_{2k+1}(z)=\hat{\sigma}_{2k+2}(z).$$

这证明了定理 3 对于 $2k+2$ 也成立.

根据数学归纳法,定理 3 成立.

基于定理 3, 二元 BCH 码的译码算法的第二步中求找错位多项式的迭代算法可以化简如下:

求找错位多项式的迭代算法($q=2$) 设收到的字 $\mathbf{r}$ 的校验子

$$s_1,\ s_2,\ \cdots,\ s_{2t}$$

已算出,而
$$s_1=s_2=\cdots=s_{n_0-1}=0,\quad s_{n_0}\neq 0,$$

那么 n_0 一定是奇数. 令 $n_0=2k_0+1$. 对 k 用数学归纳法来定义一系列的线性移位寄存器

$$\langle\sigma_{2k}(z),\ l_{2k}\rangle,\quad k=1,\ 2,\ \cdots,\ t.$$

(1) 令
$$\sigma_2(z)=\sigma_4(z)=\cdots=\sigma_{2k_0}(z)=1,$$

$$l_2=l_4=\cdots=l_{2k_0}=0,$$

$$\sigma_{2(k_0+1)}(z)=1+d_{2k_0}z^{2k_0+1},\quad l_{2(k_0+1)}=2k_0+1,$$

其中
$$d_{2k_0}=s_{2k_0+1}.$$

(2) 设 $\langle\sigma_{2i}(z),\ l_{2i}\rangle$ 对 $i=1,\ 2,\ \cdots,\ k(k_0+1\leqslant k<t)$ 已

求得，而

$$l_2=l_4=\cdots=l_{2k_0}=0<l_{2(k_0+1)}\leqslant l_{2(k_0+2)}\leqslant\cdots\leqslant l_{2k}.$$

令 $$\sigma_{2k}(z)=1+\sigma_{2k,1}z+\sigma_{2k,2}z^2+\cdots+\sigma_{2k,l_{2k}}z^{l_{2k}}.$$

计算 $$d_{2k}=s_{2k+1}+\sigma_{2k,1}s_{2k}+\sigma_{2k,2}s_{2k-1}+\cdots+\sigma_{2k,l_{2k}}s_{2k-l_{2k}+1}.$$

区别下面两个情形：

2.1) $d_{2k}=0$. 令

$$\sigma_{2(k+1)}(z)=\sigma_{2k}(z),\quad l_{2(k+1)}=l_{2k}.$$

2.2) $d_{2k}\neq 0$. 则有 $m(0\leqslant m<k)$ 使

$$l_{2m}<l_{2(m+1)}=l_{2(m+2)}=\cdots=l_{2k}.$$

那么令 $$\sigma_{2(k+1)}(z)=\sigma_{2k}(z)-d_{2k}d_{2m}^{-1}z^{2(k-m)}\sigma_{2m}(z),$$

$$l_{2(k+1)}=\max\{l_{2k},\ 2k+1-l_{2k}\}.$$

最后我们得到 $\langle\sigma_{2t}(z),\ l_{2t}\rangle$. 如果 $\mathbf{r}$ 的错位个数 $e\leqslant t$, 那么 $\sigma_{2t}(z)$ 就是找错位多项式 $\sigma(z)$.

我们再指出，采用第三章 §8 中修饰的综合算式，可以避免上面这个算法中求逆元素的运算.

修饰的求找错位多项式的迭代算法$(q=2)$ 设收到的字 $\mathbf{r}$ 的校验子

$$s_1,\ s_2,\ \cdots,\ s_{2t}$$

已算出，而 $$s_1=s_2=\cdots=s_{n_0-1}=0,\quad s_{n_0}\neq 0,$$

那么 n_0 一定是奇数. 令 $n_0=2k_0+1$. 对 k 用数学归纳法来定义一系列的多项式 $\tau_{2i}(z)$ 和一系列的非负整数 $l_{2i}(i=1,\ 2,\ \cdots,\ t)$, 而

$$\partial^0\tau_{2i}(z)\leqslant l_{2i},\quad i=1,\ 2,\ \cdots,\ t.$$

(1) 令 $$\tau_2(z)=\tau_4(z)=\cdots=\tau_{2k_0}(z)=1,$$

$$l_2=l_4=\cdots=l_{2k_0}=0,$$

$$\tau_{2(k_0+1)}(z)=1+D_{2k_0}z^{2k_0+1},\quad l_{2(k_0+1)}=2k_0+1,$$

其中 $$D_{2k_0}=s_{2k_0+1}.$$

(2) 设 $\tau_{2i}(z)$, l_{2i} 对 $i=1,\ 2,\ \cdots,\ k(k_0+1\leqslant k<t)$ 已求

得，而

$$\partial^0 \tau_{2i}(z) \leqslant l_{2i},$$

$$l_2 = l_4 = \cdots = l_{2k_0} = 0 < l_{2(k_0+1)} \leqslant l_{2(k_0+2)} \leqslant \cdots \leqslant l_{2k}.$$

令 $$\tau_{2k}(z) = \tau_{2k,0} + \tau_{2k,1}z + \tau_{2k,2}z^2 + \cdots + \tau_{2k,l_{2k}}z^{l_{2k}}.$$

计算

$$D_{2k} = \tau_{2k,0}s_{2k+1} + \tau_{2k,1}s_{2k} + \tau_{2k,2}s_{2k-1} + \cdots + \tau_{2k,l_{2k}}s_{2k-l_{2k}+1}.$$

区别下面两个情形:

2.1) $D_{2k}=0$. 令

$$\tau_{2k+2}(z) = \tau_{2k}(z), \quad l_{2k+2} = l_{2k}.$$

2.2) $D_{2k} \neq 0$. 那么有 $m(1 \leqslant m < k)$ 使

$$l_{2m} < l_{2(m+1)} = l_{2(m+2)} = \cdots = l_{2k}.$$

那么令 $$\tau_{2(k+1)}(z) = D_{2m}\tau_{2k}(z) - D_{2k}z^{2(k-m)}\tau_{2m}(z),$$

$$l_{2(k+1)} = \max\{l_{2k},\ 2k+1-l_{2k}\}.$$

最后我们得到 $\tau_{2t}(z)$. 根据第三章 § 8 定理 4 可知,

$$\tau_{2t}(z) = \tau_{2t,0}\sigma_{2t}(z), \quad \tau_{2t,0} \in \mathbf{F}_{2^r}^*.$$

既然 $\tau_{2t}(z)$ 和 $\sigma_{2t}(z)$ 只差 $\mathbf{F}_{2^r}^*$ 中的一个因子，所以它们有相同的根. 因此我们不必去求 $\sigma_{2t}(z)$ 的根，而去求 $\tau_{2t}(z)$ 的根就行了，这样就可以得到错位.

最后我们再指出 q 元 BCH 码可作如下的推广， 仍设 α 是 $\mathbf{F}_q$ 上的一个 n 阶元, $(n, q)=1$, 而 q 在 $\mathbf{Z}_n^*$ 中的阶是 r, 设 m_0 是个正整数, d 是个整数而 $2 \leqslant d \leqslant n-1$, 那么

$$\alpha^{m_0},\ \alpha^{m_0+1},\ \alpha^{m_0+2},\ \cdots,\ \alpha^{m_0+d-2}.$$

这 d_0-1 个元素两两相异. 我们构造一个 $r(d-1)\times n$ 矩阵

$$\begin{pmatrix} 1 & \alpha^{m_0} & (\alpha^{m_0})^2 & \cdots & (\alpha^{m_0})^{n-1} \\ 1 & \alpha^{m_0+1} & (\alpha^{m_0+1})^2 & \cdots & (\alpha^{m_0+1})^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{m_0+d-2} & (\alpha^{m_0+d-2})^2 & \cdots & (\alpha^{m_0+d-2})^{n-1} \end{pmatrix},$$

我们把以这个矩阵为校验矩阵的码长 n 的 q 元线性码叫做设

计距离 d 的码长 n 的 q 元广义 BCH 码. 完全和定理 1 一样, 可以证明设计距离 d 的码长 n 的 q 元广义 BCH 码是循环群, 它的生成多项式是 $\mathbf{F}_q$ 上以 α^{m_0}, α^{m_0+1}, α^{m_0+2}, $\cdots$, α^{m_0+d-2} 为根的次数最低的多项式. 完全和定理 2 一样, 可以证明它的极小距离 $\geqslant d$. 更进一步, 本节介绍的 q 元 BCH 码的代数译码方法完全可以推广到 q 元广义 BCH 码上来. 由于推导完全一样, 我们就都不重复了.

§6 Reed-Solomon 码

前面几节讨论的纠错码都是纠正独立差错的码. 但有时码字在信道中传送时, 特别在短波信道中传送时, 差错往往是成区间出现的, 即连续几个位的码元都发生差错, 或连续几个位的码元除其中少数几个以外都发生差错. 因此讨论纠正成区间的差错的码是有意义的. 下面将介绍的 Reed-Solomon 码就是一个比较好的纠正成区间的差错的码.

所谓 q 元 Reed-Solomon 码就是码长 $n=q-1$ 的 q 元 BCH 码, 而 $q>2$. 为了说明怎样利用它去纠正成区间的差错, 我们先给出成区间的差错模式的定义.

定义 1 设 $\mathbf{e}$ 是码长 n 的某个 q 元码的一个差错模式, 令

$$\mathbf{e}=(e_0, e_1, e_2, \cdots, e_{n-1}), \quad e_i\in\mathbf{F}_q.$$

如果 $\mathbf{e}$ 中有连续 b 个位, 譬如第 m_0+1 位, 第 m_0+2 位, $\cdots$, 第 m_0+b 位, 使得

$$e_j=0, \text{ 当 } j<m_0+1, \text{ 或 } j>m_0+b \text{ 时},$$

$$e_{m_0+1}\neq 0,$$

$$e_{m_0+b}\neq 0,$$

我们就说 $\mathbf{e}$ 是一个长为 b 的成区间的差错模式. 设发方发出

的码字是 $\mathbf{c}$，收方收到的字是 $\mathbf{r}$．如果 $\mathbf{r}-\mathbf{c}$ 是一个长为 b 的成区间的差错模式，我们就说 $\mathbf{c}$ 在信道中传输时出现了一个长为 b 的成区间的差错．

首先，容易证明下面这个定理．

定理 1 q 元 (n, k) 循环码可以检查出任一长 $b\leqslant n-k$ 的成区间差错．

证．设 $\mathbf{c}$ 是发方发送的一个码字，而 $\mathbf{c}$ 在传送过程中出现了一个长 $b\leqslant n-k$ 的成区间差错 $\mathbf{e}$．令

$$\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{n-1}),$$

$$\mathbf{e}=(e_0, e_1, e_2, \cdots, e_{n-1}),$$

那么 $\mathbf{e}$ 中有连续 b 个位：第 m_0+1 位，第 m_0+2 位，…，第 m_0+b 位，使得

$$e_j=0, \text{ 如果 } j<m_0+1 \text{ 或 } j>m_0+1,$$

$$e_{m_0+1}\neq 0, \quad e_{m_0+b}\neq 0.$$

于是 $\quad e(x)=e_0+e_1x+e_2x^2+\cdots+e_{n-1}x^{n-1}=x^{m_0+1}a(x),$

而 $\quad a(x)=e_{m_0+1}+e_{m_0+2}x+\cdots+e_{m_0+b}x^{b-1},$

那么 $\quad \partial^0 a(x)=b-1\leqslant n-k-1.$

设 $g(x)$ 是这个 (n, k) 循环码的生成多项式，那么

$$\partial^0 g(x)=n-k.$$

因此 $\quad g(x)\nmid a(x).$

又因 $g(x)$ 的零次项不等于 0，所以

$$g(x)\nmid e(x).$$

因 $\mathbf{c}$ 是码字，所以

$$g(x)\mid c(x)=c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}.$$

那么 $\quad g(x)\nmid c(x)+e(x).$

这就是说，收方收到的字 $\mathbf{c}+\mathbf{e}$ 不是码字．因而收方可以检查出码字 $\mathbf{c}$ 在传送过程中发生差错．

设 q 是一个素数的幂，并假定 $q>2$．今考察设计距离 d

的码长 $q-1$ 的 q 元 Reed-Solomon 码，将它记作 C。设 α 是 $\mathbf{F}_q$ 的一个本原元，那么 C 的生成多项式就是

$$g(x)=\prod_{i=1}^{d-1}(x-\alpha^i).$$

根据 §5 定理 2，C 的极小距离 $\geqslant d$. 更进一步，我们证明

定理 2 设计距离 d 的码长 $q-1$ 的 q 元 Reed-Solomon 码的极小距离等于 d.

证. 令

$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{q-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \cdots & (\alpha^{d-1})^{q-2} \end{pmatrix},$$

那么 $\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{q-2})\in C$，当且仅当

$$H\mathbf{c}'=\mathbf{0}.$$

因 H 的任意 $d-1$ 个列线性无关，所以 H 的秩是 $d-1$. 那么 H 的任意 d 列线性相关，这就是说 C 有重量等于 d 的码字，因此 C 的极小距离等于 d.

系理 设计距离 d 的码长 $n=q-1$ 的 q 元 Reed-Solomon 码的码长 n，信息位的个数 k 和极小距离 d 三者之间适合关系式

$$d=n-k+1.$$

证. 因 $\partial^0 g(x)=d-1$，所以

$$k=n-(d-1)=n-d+1.$$

注意，一般说来，我们有

定理 3 (n, k)线性码的极小距离 $d\leqslant n-k+1$.

证. 设 (n, k) 线性码 C 的校验矩阵 H 是秩为 $n-k$ 的 $(n-k)\times n$ 矩阵. 因此 H 的任意 $n-k+1$ 列必线性相关. 这就是说 C 中一定有重量 $n-k+1$ 的码字. 因此

$$d \leqslant n-k+1.$$

基于定理 3，我们可以给出下面的定义

定义 2 设有一(n, k)线性码，它的极小距离 d 达到极大值 $n-k+1$，即 $d=n-k+1$，我们就说这个(n, k)线性码是**极大距离可分码，或最优码**.

有了定义 2，那么定理 2 的系理实际上是说 Reed-Solomon 码是极大距离可分码.

注意，当 n 和 k 给定时，码长 n 而信息位个数等于 k 的线性码中极大距离可分码是纠错能力最大的码.

下面我们介绍怎样利用 Reed-Solomon 码来纠正成区间的差错.

设 $q=2^r$，而 $r>1$. 仍设 α 是 $\mathbf{F}_q$ 的一个本原元，那么 $1, \alpha, \alpha^2, \cdots, \alpha^{r-1}$ 就组成 $\mathbf{F}_q$ 在 $\mathbf{F}_2$ 上的一组基. 于是 $\mathbf{F}_q$ 中任一元素 a 都可以唯一地表成 $1, \alpha, \alpha^2, \cdots, \alpha^{r-1}$ 的线性组合，而系数属于 $\mathbf{F}_2$:

$$a=\sum_{i=0}^{r-1} a_i \alpha^i, \quad a_i \in \mathbf{F}_2. \tag{1}$$

这样 $\mathbf{F}_q$ 中每一元素 a 都唯一地确定了 $\mathbf{F}_2$ 上的一个 r 维行向量

$$(a_0, a_1, a_2, \cdots, a_{r-1}). \tag{2}$$

仍设 C 是设计距离 d 的码长 $q-1$ 的 q 元 Reed-Solomon 码，并假定 $d=2t+1$. 根据定理 2，C 的信息位的个数

$$k=n-2t.$$

再设
$$\mathbf{c}=(c_0, c_1, c_2, \cdots, c_{q-2})$$
是 C 的任意一个码字，$\mathbf{c}$ 的每个码元 $c_i(0 \leqslant i \leqslant q-2)$ 都是 $\mathbf{F}_q$ 中的元素. 每个 c_i 都按上述 (1)，(2) 式唯一确定 $\mathbf{F}_2$ 上的一个 r 维行向量，将每个 c_i 所唯一确定的 $\mathbf{F}_2$ 上的 r 维行向量代入 $\mathbf{c}$，就得到 $\mathbf{F}_2$ 上的一个 $(q-1)r$ 维行向量. 这些行

向量的全体组成一个码长 $(q-1)r$ 的二元线性码，记作 C'. 在数字通信中采用 C' 作为纠错码，就可以纠正一个长 $b\leqslant(t-1)r+1$ 的成区间差错. 实际上，长 $b\leqslant(t-1)r+1$ 的成区间差错模式顶多影响原来码 C 中连续 t 个码元，而 C 是可以纠正 t 个差错的纠错码.

当然在上面的讨论中，如果取 $q=q_0^r$，就得到可以纠正一个长 $b\leqslant(t-1)r+1$ 的成区间差错的 q_0 元码.

第五章　有限域上的多项式

在这一章里，我们要讨论编码理论里出现的，有关有限域上多项式的几个重要问题．这就是：确定有限域上多项式的周期的问题，有限域上多项式的因式分解问题，特别是 x^n-1 的因式分解问题，以及确定有限域上次数 $\leqslant$ 某一个正整数 n 的所有不可约多项式和本原多项式的问题．这些问题都是当前值得研究的问题．我们介绍的确定有限域上多项式的周期的方法和有限域上多项式的因式分解的方法，当域的元素个数较小时，特别当有限域是 $\mathbf{F}_2$ 时，而且当多项式的次数不太大时，譬如 $\leqslant 1000$ 或更大一点时，都可以编成程序在电子数字计算机上计算．

§1　辗转相除法

设 $\mathbf{F}_q$ 是 q 个元素的有限域，而 q 是一个素数幂．在编码中时常要遇到求 $\mathbf{F}_q$ 上两个不等于 0 的多项式 $a(x)$ 和 $b(x)$ 的最高公因式 $(a(x),\ b(x))$ 的问题，以及将 $(a(x),\ b(x))$ 表成 $a(x)$ 和 $b(x)$ 的以 $\mathbf{F}_q[x]$ 中的元素为系数的线性组合的问题．在第一章 §2 中我们曾经说过，这两个问题可以用辗转相除法来解决．我们回忆，辗转相除法是一串带余除法算式，见第一章 §2(3) 式，其中每一个带余除法算式

$$r_{i-2}(x)=q_i(x)r_{i-1}(x)+r_i(x),\quad \partial^0 r_i(x)<\partial^0 r_{i-1}(x),$$

的除式 $r_{i-1}(x)$ 是前一个带余除法算式的余式，而被除式 $r_{i-2}(x)$ 是更前一个带余除法算式的余式．一旦某一个带余除

法算式，譬如第 $n+1$ 个的余式等于0时，

$$r_{n-1}(x)=q_{n+1}(x)r_n(x),$$

这个带余除法算式的除式 $r_n(x)$，除可能差 $\mathbf{F}_q$ 中一个非零元素之外，就是 $a(x)$ 和 $b(x)$ 的最高公因式 $(a(x),\ b(x))$. 因此利用辗转相除法去求 $a(x)$ 和 $b(x)$ 的最高公因式，在进行每一次带余除法时，只需要记住前两次带余除法算式的余式. 用电子数字计算机来进行运算时，这需要的存储量是不大的. 可是如果要将 $a(x)$ 和 $b(x)$ 的最高公因式 $(a(x),\ b(x))$ 表成它们的以 $\mathbf{F}_q[x]$ 中元素为系数的线性组合，那就需要先将前 n 个带余除法算式的余式表成被除式和除式的线性组合：

$$r_k(x)=r_{k-2}(x)-q_k(x)r_{k-1}(x),\quad k=1,\ 2,\ \cdots,\ n.$$

然后将如此所得的 $r_{n-1}(x)$ 的表达式代入 $r_n(x)$ 的表达式就把 $r_n(x)$ 表成 $r_{n-3}(x)$ 和 $r_{n-2}(x)$ 的线性组合

$$r_n(x)=(-q_n(x))r_{n-3}(x)+(1+q_{n-1}q_n)r_{n-2}(x);$$

再将 $r_{n-2}(x)$ 的表达式代入上式就将 $r_n(x)$ 表成 $r_{n-4}(x)$ 和 $r_{n-3}(x)$ 的线性组合；如此继续下去，就可以将 $r_n(x)$ 表成 $a(x)$ 和 $b(x)$ 的线性组合. 这样每一个带余除式算式就都需要记住. 因此需要的存储量就比较大. 实际上，只要将辗转相除法稍加修饰，每进行一步计算只需要记住4个多项式，这样也可以求出 $a(x)$ 和 $b(x)$ 的最高公因式 $(a(x),\ b(x))$，并将 $(a(x),\ b(x))$ 表成 $a(x)$ 和 $b(x)$ 的以 $\mathbf{F}_q[x]$ 中元素为系数的线性组合，下面我们就来介绍这个算法*.

修饰的辗转相除法 设 $a(x)$ 和 $b(x)$ 是 $\mathbf{F}_q[x]$ 中的两个不等于0的多项式. 记

$$r_{-1}(x)=a(x),\ r_0(x)=b(x).$$

---

* 这个算法实际上就是秦九韶在大衍求一术中对于整数的情形所采用的算法，见秦九韶，数书九章(1274).

定义 $$c_{-1}(x)=1,\quad c_0(x)=0,$$
$$d_{-1}(x)=0,\quad d_0(x)=1.$$
然后按下面的规则递归地计算 $r_k(x)$, $c_k(x)$, $d_k(x)$, $k=1$, 2, 3, ….

$$\left.\begin{aligned} r_{k-2}(x)&=q_k(x)r_{k-1}(x)+r_k(x),\ \partial^0 r_k(x)<\partial^0 r_{k-1}(x),\\ c_k(x)&=q_k(x)c_{k-1}(x)+c_{k-2}(x),\\ d_k(x)&=q_k(x)d_{k-1}(x)+d_{k-2}(x).\end{aligned}\right\}\quad(1)$$

直到 $r_{n+1}(x)=0$ 时停止. 那么除了可能差 $\mathbf{F}_q^*$ 中一个元素以外, $r_n(x)$ 就是 $a(x)$ 和 $b(x)$ 的最高公因式 $(a(x),\ b(x))$, 而

$$r_n(x)=(-1)^n c_n(x)a(x)+(-1)^{n+1}d_n(x)b(x).\quad(2)$$

定理 1 设 $a(x)$ 和 $b(x)$ 是 $\mathbf{F}_q[x]$ 中的两个不等于 0 的多项式, 那么按修饰的辗转相除法计算, 当 $r_{n+1}(x)=0$ 时, $r_n(x)$ 确实除了可能差一个 $\mathbf{F}_q^*$ 的元素之外, 就是 $a(x)$ 和 $b(x)$ 的最高公因式; 而且

$$r_n(x)=(-1)^n c_n(x)a(x)+(-1)^{n+1}d_n(x)b(x)\quad(2)$$

证. 设 $r_n(x)$ 的首项系数是 c, 那么和附录二中关于整数的情形完全一样, 可以证明

$$(a(x),\ b(x))=c^{-1}r_n(x).$$

我们就不重复了. 主要的问题是去证明(2).

首先, 容易验证

$$\begin{aligned} &c_k(x)r_{k+1}(x)+c_{k+1}(x)r_k(x)\\ &\quad=c_k(x)(r_{k-1}(x)-q_{k+1}(x)r_k(x))\\ &\qquad+(q_{k+1}(x)c_k(x)+c_{k-1}(x))r_k(x)\\ &\quad=c_{k-1}(x)r_k(x)+c_k(x)r_{k-1}(x),\end{aligned}\quad(3)$$

$$\begin{aligned} &d_k(x)r_{k+1}(x)+d_{k+1}(x)r_k(x)\\ &\quad=d_k(x)(r_{k-1}(x)-q_{k+1}(x)r_k(x))\\ &\qquad+(q_{k+1}(x)d_k(x)+d_{k-1}(x))r_k(x)\\ &\quad=d_{k-1}(x)r_k(x)+d_k(x)r_{k-1}(x),\end{aligned}\quad(4)$$

$$c_k(x)d_{k+1}(x)-c_{k+1}(x)d_k(x)$$
$$=c_k(x)(q_{k+1}(x)d_k(x)+d_{k-1}(x))$$
$$-(q_{k+1}(x)c_k(x)+c_{k-1}(x))d_k(x)$$
$$=-(c_{k-1}(x)d_k(x)-c_k(x)d_{k-1}(x)).\qquad(5)$$

其次,对 k 用数学归纳法,并利用(3),(4),(5)式,可以证明

$$\left.\begin{array}{l}d_k(x)r_{k-1}(x)+d_{k-1}(x)r_k(x)=r_{-1}(x),\\ c_k(x)r_{k-1}(x)+c_{k-1}(x)r_k(x)=r_0(x),\\ c_{k-1}(x)d_k(x)-c_k(x)d_{k-1}(x)=(-1)^{k+1},\end{array}\right\}\text{对 } k\geqslant 0.\qquad(6)$$

因 $r_{n+1}(x)=0$, 在(6)式中令 $k=n+1$, 就有

$$d_{n+1}(x)r_n(x)=r_{-1}(x)=a(x),\qquad(7)$$
$$c_{n+1}(x)r_n(x)=r_0(x)=b(x),\qquad(8)$$
$$c_n(x)d_{n+1}(x)-c_{n+1}(x)d_n(x)=(-1)^n.\qquad(9)$$

将(9)式双方乘以 $r_n(x)$,再利用(7),(8)两式,就得到

$$c_n(x)a(x)-d_n(x)b(x)=(-1)^n r_n(x),$$

即 $$r_n(x)=(-1)^n c_n(x)a(x)+(-1)^{n+1}d_n(x)b(x).$$

系理. 在定理1的假设下更假定 $\partial^0 a(x)>0$, $\partial^0 b(x)>0$ 而 $a(x)\neq cb(x)$ 对任一 $c\in\mathbf{F}_q$, 那么

$$\partial^0 c_n(x)<\partial^0 b(x)-\partial^0(a(x),\ b(x)),$$
$$\partial^0 d_n(x)<\partial^0 a(x)-\partial^0(a(x),\ b(x)).$$

证. 显然有

$$\partial^0 q_k(x)>0,\ k=1,\ 2,\ \cdots,\ n+1,$$

那么由(1)中第二式得

$$\partial^0 c_{k-1}(x)<\partial^0 c_k(x),\ k=1,\ 2,\ \cdots,\ n+1,$$

特别 $$\partial^0 c_n(x)<\partial^0 c_{n+1}(x).$$

由(8)式得 $$\partial^0 c_{n+1}(x)=\partial^0 b(x)-\partial^0 r_n(x).$$

因此 $$\partial^0 c_n(x)<\partial^0 b(x)-\partial^0(a(x),\ b(x)).$$

同理 $$\partial^0 d_n(x)<\partial^0 a(x)-\partial^0(a(x),\ b(x)).$$

我们举一个例子. 设

$$a(x)=x^5+x^4+x^3+x^2+x+1,$$
$$b(x)=x^4+x^2+x+1$$

是 $\mathbf{F}_2$ 上的多项式．现在用修饰的辗转相除法去求它们的最高公因式 $(a(x),\ b(x))$，并将它表成 $a(x)$ 和 $b(x)$ 的线性组合．

首先，令

$$r_{-1}(x)=a(x)=x^5+x^4+x^3+x^2+x+1,$$
$$r_0(x)=b(x)=x^4+x^2+x+1,$$
$$c_{-1}(x)=1,\ c_0(x)=0,$$
$$d_{-1}(x)=0,\ d_0(x)=1.$$

第一步，用 $r_0(x)$ 去除 $r_{-1}(x)$，得

$$r_{-1}(x)=q_1(x)r_0(x)+r_1(x),$$
$$q_1(x)=x+1,\ r_1(x)=x^2+x.$$

接着计算 $$c_1(x)=q_1(x)c_0(x)+c_{-1}(x)=1,$$
$$d_1(x)=q_1(x)d_0(x)+d_{-1}(x)=x+1.$$

第二步，再用 $r_1(x)$ 去除 $r_0(x)$，得

$$r_0(x)=q_2(x)r_1(x)+r_2(x),$$
$$q_2(x)=x^2+x,\ r_2(x)=x+1.$$

接着计算 $$c_2(x)=q_2(x)c_1(x)+c_0(x)=x^2+x,$$
$$d_2(x)=q_2(x)d_1(x)+d_0(x)=x^3+x+1.$$

第三步，再用 $r_2(x)$ 去除 $r_1(x)$，得

$$r_1(x)=q_3(x)r_2(x),\ q_3(x)=x.\ r_3(x)=0.$$

因 $r_3(x)=0$，计算就停止．我们有

$$(a(x),\ b(x))=r_2(x)=x+1.$$

又有

$$\begin{aligned}(a(x),\ b(x))&=c_2(x)a(x)+d_2(x)b(x)\\&=(x^2+x)(x^5+x^4+x^3+x^2+x+1)\\&\quad+(x^3+x+1)(x^4+x^2+x+1).\end{aligned}$$

§2 确定多项式的周期的一个方法

设 $\mathbf{F}_q$ 是 q 个元素的有限域，而 q 是一个素数 p 的幂．再设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个次数 $\geqslant 1$ 的多项式，而 $f(0)\neq 0$．在第三章 §2 定义 3 里，我们曾经定义了 $f(x)$ 的周期为最小正整数 l 使 $f(x)\mid x^l-1$，并用 $p(f)$ 来代表 $f(x)$ 的周期．我们也曾指出 $f(x)$ 的周期 $p(f)$ 也等于 x 在乘法交换群 $\mathbf{F}_q[x]^*_{f(x)}$ 中的阶．同时我们在第三章 §2 定理 4 里还证明了，以 $f(x)$ 为极小多项式的线性移位寄存器序列的周期就等于 $f(x)$ 的周期．特别，当 $f(x)$ 是零次项不等于 0 的不可约多项式时，$f(x)$ 所产生的非零线性移位寄存器序列的周期都等于 $f(x)$ 的周期．另一方面，根据第四章 §3 定理 1 我们知道，以 $\mathbf{F}_q$ 上的一个次数 $\geqslant 1$ 的零次项不等于 0 的 $f(x)$ 为生成多项式的 q 元循环码的码长的极小值也是 $f(x)$ 的周期．因此确定 $\mathbf{F}_q[x]$ 中次数 $\geqslant 1$ 的零次项不等于 0 的多项式 $f(x)$ 的周期是有意义的．

下面我们要介绍一个求 $\mathbf{F}_q[x]$ 中次数 $\geqslant 1$ 的零次项不等于 0 的多项式 $f(x)$ 的周期的方法．我们先回忆，在第三章 §2 中我们曾经证明过的一个引理．

引理 1 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中次数 $\geqslant 1$ 的零次项不等于 0 的一个多项式．用 $p(f)$ 表示 $f(x)$ 的周期．如果 $f(x)\mid x^l-1$，那么 $p(f)\mid l$．

这是第三章 §2 的引理 3．

我们再证明几条引理．

引理 2 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中零次项不等于 0 的多项式，并假定

$$f(x)=f_1(x)f_2(x),\ \partial^0 f_1(x),\ \partial^0 f_2(x)\geqslant 1$$

而 $$(f_1(x), f_2(x))=1,$$
那么 $f(x)$ 的周期 $p(f)$ 就等于 $f_1(x)$ 的周期 $p(f_1)$ 与 $f_2(x)$ 的周期 $p(f_2)$ 的最小公倍数 $[p(f_1), p(f_2)]$，即
$$p(f)=[p(f_1), p(f_2)].$$
证. 我们有
$$f_1(x)\mid x^{p(f_1)}-1,\ f_2(x)\mid x^{p(f_2)}-1.$$
设 $l=[p(f_1), p(f_2)]$，那么
$$x^{p(f_1)}-1\mid x^l-1,\ x^{p(f_2)}-1\mid x^l-1.$$
因此 $$f_1(x)\mid x^l-1,\ f_2(x)\mid x^l-1.$$
但是 $(f_1(x), f_2(x))=1$，所以
$$f_1(x)f_2(x)\mid x^l-1,$$
即 $$f(x)\mid x^l-1.$$
因此根据引理 1 有
$$p(f)\mid l.$$
另一方面，从
$$f(x)\mid x^{p(f)}-1$$
推出 $$f_1(x)\mid x^{p(f)}-1,\ f_2(x)\mid x^{p(f)}-1.$$
仍根据引理 1 有
$$p(f_1)\mid p(f),\ p(f_2)\mid p(f).$$
于是 $p(f_1)$ 和 $p(f_2)$ 的最小公倍数 l 也是 $p(f)$ 的因数，即
$$l\mid p(f).$$
那么从 $p(f)\mid l$ 和 $l\mid p(f)$ 推出
$$p(f)=l=[p(f_1), p(f_2)].$$
引理 3 设 $(j, p)=1$，那么 $\mathbf{F}_q[x]$ 中的多项式 x^j-1 没有重因式.

证. 令 $$f(x)=x^j-1,$$
那么 $$f'(x)=jx^{j-1}.$$
因 $(j, p)=1$ 而 p 为 $\mathbf{F}_q$ 的特征，所以 $f'(x)\neq 0$. $f'(x)$ 的不可

约因式只有x，而

$$x \nmid x^j - 1.$$

所以 $$(f(x), f'(x)) = 1.$$

那么根据第一章§2定理3可知$f(x) = x^j - 1$没有重因式.

引理4 设$f(x)$是$\mathbf{F}_q[x]$中的不可约多项式而$f(0) \neq 0$. 再设e是$\geqslant 0$的整数. 用$p(f)$表$f(x)$的周期，用$p(f^e)$表示$f(x)^e$的周期. 那么

$$p(f^e) = p(f) \cdot \min\{p^i \mid p^i \geqslant e\}.$$

$\min\{p^i \mid p^i \geqslant e\}$表示$\geqslant e$的$p$的最小的幂.

证. 设 $$\min\{p^i \mid p^i \geqslant e\} = p^m,$$

即 $$p^m \geqslant e \text{ 而 } p^{m-1} < e.$$

从 $$f(x) \mid x^{p(f)} - 1$$

推出 $$f(x)^e \mid (x^{p(f)} - 1)^e.$$

但是 $$(x^{p(f)} - 1)^e \mid (x^{p(f)} - 1)^{p^m},$$

所以 $$f(x)^e \mid (x^{p(f)} - 1)^{p^m}.$$

因$\mathbf{F}_q$的特征为p，

$$(x^{p(f)} - 1)^{p^m} = x^{p(f) \cdot p^m} - 1.$$

于是

$$p(f^e) \mid p(f) \cdot p^m. \tag{1}$$

另一方面，设

$$p(f^e) = k.$$

写 $$k = p^i \cdot j \text{ 而 } (j, p) = 1.$$

那么 $$f(x)^e \mid x^{p^i \cdot j} - 1 = (x^j - 1)^{p^i}.$$

根据引理3，$x^j - 1$没有重因式. 又因$f(x)$是不可约多项式，所以根据唯一因式分解定理(第一章§2定理3)推出

$$f(x) \mid x^j - 1, \text{ 而 } e \leqslant p^i.$$

再根据引理1，从$f(x) \mid x^j - 1$推出

$$p(f) \mid j.$$

因此

$$k=p^t j\geqslant p^m\cdot p(f). \tag{2}$$

从(1), (2)两式可推出

$$p(f^e)=p(f)\cdot p^m=p(f)\cdot\min\{p^t|p^t\geqslant e\}.$$

引理 5 设 $f(x)$是 $\mathbf{F}_q[x]$中的不可约多项式而$f(0)\neq 0$. 用 $p(f)$ 表示$f(x)$ 的周期,那么

$$(p(f),\ p)=1.$$

证. 设 $f(x)$是 n 次不可约多项式,那么 $n\geqslant 1$. 从第一章§5引理 2, 知

$$f(x)\,|\,x^{q^n}-x.$$

又因 $f(0)\neq 0$, 即 $f(x)\neq x$, 所以

$$f(x)\,|\,x^{q^n-1}-1.$$

那么根据引理 1 有

$$p(f)\,|\,q^n-1.$$

因 $(q^n-1,\ p)=1$, 所以

$$(p(f),\ p)=1.$$

从上面这些引理立刻可以推出

定理 1 设 $f(x)$ 是 $\mathbf{F}_q[x]$中零次项不等于 0 的一个多项式,并假定

$$f(x)=f_1(x)^{e_1}f_2(x)^{e_2}\cdots f_r(x)^{e_r},$$

其中 $f_1(x),\ f_2(x),\ \cdots,\ f_r(x)$ 是 $\mathbf{F}_q[x]$ 中 r 个两两不同的不可约多项式,而 $e_1,\ e_2,\ \cdots,\ e_r$ 是 r 个正整数,那么

$$\begin{aligned}p(f)=&[p(f_1),\ p(f_2),\ \cdots,\ p(f_r)]\\&\cdot\min\{p^t|p^t\geqslant e_1,\ e_2,\ \cdots,\ e_r\}.\end{aligned}$$

证. 根据引理 2, 用归纳法向 r 可得

$$\begin{aligned}p(f)&=[p(f_1^{e_1}),\ p(f_2^{e_2}\cdots f_r^{e_r})]\\&=[p(f_1^{e_1}),\ [p(f_2^{e_2}),\ \cdots,\ p(f_r^{e_r})]]\\&=[p(f_1^{e_1}),\ p(f_2^{e_2}),\ \cdots,\ p(f_r^{e_r})]\end{aligned}$$

再根据引理 4，有

$$p(f_i^{e_i})=p(f_i)\cdot\min\{p^t\,|\,p^t\geqslant e_i\},\ i=1,\ 2,\ \cdots,\ r.$$

又根据引理 5，$(p(f_i),\ p)=1$，所以

$$p(f)=[p(f_1),\ p(f_2),\ \cdots,\ p(f_r)]\cdot\min\{p^t\,|\,p^t\geqslant e_1,\ e_2,\ \cdots,\ e_r\}.$$

这证明了定理 1.

根据定理 1，要确定 $\mathbf{F}_q[x]$ 中一个次数 $\geqslant 1$ 的零次项不等于 0 的多项式 $f(x)$ 的周期，可以分两步走. 第一步是把 $f(x)$ 分解成 $\mathbf{F}_q[x]$ 中不可约多项式的乘积，或把 $f(x)$ 表成 $\mathbf{F}_q[x]$ 中有限个两两不同的不可约多项式的幂的乘积. 关于这个问题，下一节将要介绍一个一般的因式分解的方法，第二步是要确定 $f(x)$ 的不可约因式的周期. 下面我们介绍一个确定 $\mathbf{F}_q[x]$ 中零次项不等于 0 的不可约多项式的周期的方法.

现在设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个 n 次不可约多项式，并假定 $f(x)\neq x$，即 $f(x)$ 的零次项 $\neq 0$. 那么确定 $f(x)$ 的周期可以按以下步骤进行：

1) 将 q^n-1 分解成素数的乘积，设

$$q^n-1=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r},$$

其中 $p_1,\ p_2,\ \cdots,\ p_r$ 是 r 个两两不同的素数，而 $e_1,\ e_2,\ \cdots,\ e_r$ 是 r 个正整数.

2) 对每个 $i=1,\ 2,\ \cdots,\ r$，计算

$$\left(x^{(q^n-1)/r_i}\right)_{f(x)},\ \left(x^{(q^n-1)/p_i^2}\right)_{f(x)},\ \left(x^{(q^n-1)/p_i^3}\right)_{f(x)},\ \cdots$$

直到求得一个非负整数 $f_i\leqslant e_i$

$$\left(x^{(q^n-1)/p_i^{f_i}}\right)_{f(x)}=1,\ \left(x^{(q^n-1)/p_i^{f_i+1}}\right)_{f(x)}\neq 1.$$

（注意，我们仍沿用第一章 § 2 中的记号，将用 $f(x)$ 去除 $a(x)$ 所得的余式记作 $(a(x))_{f(x)}$. 我们还约定 $\left(x^{(q^n-1)/p_i^{e_i+1}}\right)_{f(x)}\neq 1$.）那么

$$p(f) \mid (q^n-1)/p_i^{f_i},\ p(f) \nmid (q^n-1)/p_i^{f_i+1}.$$

因此
$$p(f) = p_1^{e_1-f_1} p_2^{e_2-f_2} \cdots p_r^{e_r-f_r}$$

在计算

$$(x^{(q^n-1)/p_i^s})_{f(x)},\ s=1,\ 2,\ \cdots;\ i=1,\ 2,\ \cdots,\ r$$

时，可以按以下步骤进行：

2.1) 计算

$$(x^0)_{f(x)},\ (x^q)_{f(x)},\ (x^{2q})_{f(x)},\ \cdots,\ (x^{(n-1)q})_{f(x)}.$$

设
$$(x^{jq})_{f(x)} = \sum_{i=0}^{n-1} a_{ij} x^i,\ j=0,\ 1,\ 2,\ \cdots,\ n-1.$$

令
$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} & \cdots & a_{0n-1} \\ a_{10} & a_{11} & a_{12} & \cdots & a_{1n-1} \\ a_{20} & a_{21} & a_{22} & \cdots & a_{2n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n-10} & a_{n-11} & a_{n-12} & \cdots & a_{n-1n-1} \end{pmatrix}.$$

A 是 $\mathbf{F}_q$ 上的一个 $n\times n$ 矩阵.

2.2) 计算

$$(x)_{f(x)},\ (x^q)_{f(x)},\ (x^{q^2})_{f(x)},\ \cdots,\ (x^{q^{n-1}})_{f(x)}.$$

注意，当 $q^i \leqslant (n-1)q$ 时，$q^i = (q^{i-1})q$ 而 $q^{i-1} \leqslant n-1$. 因此 $(x^{q^i})_{f(x)}$ 在第 2.1) 步中已算出.

又，如果 $(x^{q^i})_{f(x)}$ 已算出，设

$$(x^{q^i})_{f(x)} = \sum_{j=0}^{n-1} b_j x^j,$$

那么

$$\begin{aligned}(x^{q^{i+1}})_{f(x)} &= (\underbrace{x^{q^i}\cdot x^{q^i}\cdot\cdots\cdot x^{q^i}}_{q\text{个}})_{f(x)} \\ &= ((\underbrace{(x^{q^i})_{f(x)}\cdot (x^{q^i})_{f(x)}\cdot\cdots\cdot (x^{q^i})_{f(x)}}_{q\text{个}})_{f(x)} \\ &= (((x^{q^i})_{f(x)})^q)_{f(x)} = \left(\left(\sum_{j=0}^{n-1} b_j x^j\right)^q\right)_{f(x)}\end{aligned}$$

$$=\left(\sum_{j=0}^{n-1} b_j x^{jq}\right)_{f(x)} = \sum_{j=0}^{n-1} b_j (x^{jq})_{f(x)}$$

$$=\sum_{j=0}^{n-1} b_j \sum_{i=0}^{n-1} a_{ij} x^i.$$

$$=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1} a_{ij} b_j\right) x^i.$$

这就是说，如令

$$(x^{q^{i+1}})_{f(x)} = \sum_{j=0}^{n-1} b'_j x^j,$$

那么

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ \vdots \\ b'_{n-1} \end{pmatrix} = A \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{pmatrix}.$$

令 $$g_i(x) = (x^{q^i})_{f(x)},\quad i=0,\ 1,\ 2,\ \cdots,\ n-1.$$

2.3) 将 $(q^n-1)/p_i^s$ 表成 q 进位数. 设

$$(q^n-1)/p_i^s = a_0 + a_1 q + a_2 q^2 + \cdots + a_{n-1} q^{n-1},$$
$$0 \leqslant a_i \leqslant q-1.$$

2.4) 计算

$$(x^{(q^n-1)/p_i^s})_{f(x)} = \left((g_0(x)^{a_0})_{f(x)} \cdot (g_1(x)^{a_1})_{f(x)} \cdot (g_2(x)^{a_2})_{f(x)} \cdots (g_{n-1}(x)^{a_{n-1}})_{f(x)}\right)_{f(x)}.$$

我们着重指出，上面的算法，除了第一步中将 q^n-1 分解成素数的乘积以外，其余各步都不复杂，而且都可以编成程序在电子数字计算机上进行计算. 但是将 q^n-1 分解成素数的乘积这一问题，当 q 和 n 适当大时，却是相当困难的问题. 既使当 $q=2$ 时，2^n-1 的素因数分解问题，当 n 适当大时，也相当困难. 书后附有 $n\leqslant 100$ 时，2^n-1 的素因数分解表.

我们再指出，第 2.1 步和 2.2 步的计算可以用将域 $\mathbf{F}_q[x]_{f(x)}$ 中的元素乘以 x 的电路来实现：为简单起见，考察

$q=2$ 的情形．设

$$f(x)=1+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n,$$

并假定

$$c_{i_1}=c_{i_2}=\cdots=c_{i_m}=1 \quad 1\leqslant i_1<i_2<\cdots<i_m\leqslant n-1$$

而其余的 $\qquad c_j=0,\ j\neq i_1,\ i_2,\ \cdots,\ i_m.$

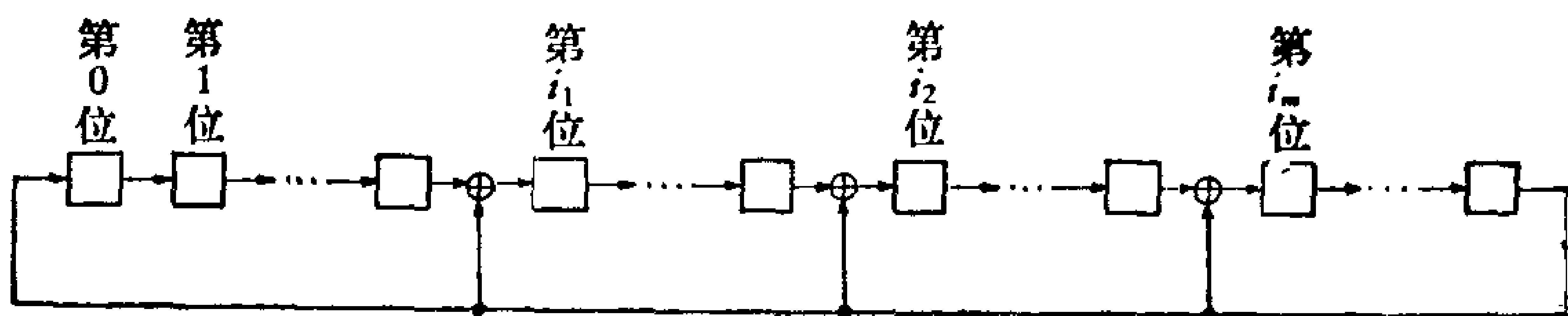


图 1

如果将上图中的这 n 个寄存器从左到右各位依序置以 a_0, a_1, a_2, $\cdots$, a_{n-1}, 这时我们说这个电路的状态是$(a_0a_1a_2\cdots a_{n-1})$, 那么加上一个移位脉冲后，这个移位寄存器的状态成为

$$(a_{n-1},\ a_0+a_{n-1}c_1,\ a_1+a_{n-1}c_2,\ \cdots,\ a_{n-2}+a_{n-1}c_{n-1}). \tag{3}$$

如果令状态$(a_0a_1a_2\cdots a_{n-1})$相应多项式

$$a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1},$$

那么加上一个移位脉冲后，这个寄存器的状态(3)就相应多项式

$$\begin{aligned}a_{n-1}&+(a_0+a_{n-1}c_1)x+(a_1+a_{n-1}c_2)x^2+\cdots\\&+(a_{n-2}+a_{n-1}c_{n-1})x^{n-1}\\&=(x(a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}))_{f(x)}.\end{aligned}$$

因此对上述移位寄存器来说，加一个移位脉冲的作用就相当于“乘以 x, 再除以 $f(x)$ 取余式的作用”．这样一来，如果令这个移位寄存器的初始状态是$(100\cdots0)$, 那么加一个移位脉冲后就得到相应于 x 的状态，加 2 个移位脉冲后使得到相应于$(x^2)_{f(x)}$ 的状态，加 4 个移位脉冲后就得到相应于$(x^4)_{f(x)}$的状态，$\cdots$; 一般地，加 $2j$ 个移位脉冲后就得到相应于 $(x^{2j})_{f(x)}$ 的状态，$j=0,\ 1,\ 2,\ \cdots,\ n-1$; 而加 2^i 个移位脉冲后就得到

相应于$(x^{2^i})_{f(x)}$的状态，$i=0, 1, 2, \cdots, n-1$.

下面我们举几个例子来阐明本节介绍的确定次数$\geqslant 1$的零次项不等于0的多项式的周期的方法.

例 1 求$\mathbf{F}_2$上不可约多项式

$$f(x)=x^9+x+1$$

的周期.

关于多项式x^9+x+1在$\mathbf{F}_2$上的不可约性将在下一节里证明. 现在我们先把它看作不可约多项式来求它的周期.

首先，我们有

$$2^9-1=511=7\cdot 73.$$

其次，我们求出矩阵A.

$$A=\begin{pmatrix}1&0&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0&0\\0&1&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0&0\\0&0&1&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&1&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0&1\end{pmatrix}$$

利用矩阵A我们可以写出

$$\begin{aligned}
&(x^1)_{f(x)}=x,\\
&(x^2)_{f(x)}=x^2,\\
&(x^{2^2})_{f(x)}=x^4,\\
&(x^{2^3})_{f(x)}=x^8,\\
&(x^{2^4})_{f(x)}=x^7+x^8,
\end{aligned}$$

并算出

$$\begin{aligned}
&(x^{2^5})_{f(x)}=x^5+x^6+x^7+x^8,\\
&(x^{2^6})_{f(x)}=x+x^2+x^3+x^4+x^5+x^6+x^7+x^8,
\end{aligned}$$

等等.

然后我们计算

$$
\begin{aligned}
\left(x^{511/7}\right)_{f(x)} &= \left(x^{73}\right)_{f(x)} \\
&= \left(x \cdot x^{2^3} \cdot x^{2^6}\right)_{f(x)} = \left(\left(x^9\right)_{f(x)} \cdot \left(x^{2^6}\right)_{f(x)}\right)_{f(x)} \\
&= \left((x+1)\left(x+x^2+x^3+x^4+x^5\right.\right. \\
&\qquad \left.\left.+x^6+x^7+x^8\right)\right)_{f(x)} \\
&= \left(x+x^9\right)_{f(x)} = 1,
\end{aligned}
$$

$$\left(x^{511/73}\right)_{f(x)} = x^7 \neq 1.$$

因此可知 $p(f) \mid 73$ 而 $p(f) \nmid 7$. 所以 $p(f)=73$.

例 2 求 $\mathbf{F}_2$ 上多项式

$$f(x)=(x+1)^3(x^2+x+1)(x^3+x+1)$$

的周期.

容易证明

$$f_1(x)=x+1,\ f_2(x)=x^2+x+1,\ f_3(x)=x^3+x+1$$

都是 $\mathbf{F}_2$ 上的不可约多项式. 显然 $p(f_1)=1$. 因 $2^2-1=3$ 和 $2^3-1=7$ 都是素数, 所以 x^2+x+1 和 x^3+x+1 都是本原多项式. 于是 $p(f_2)=3$, $p(f_3)=7$. 那么根据定理 1 就有

$$p(f)=[p(f_1),\ p(f_2),\ p(f_3)]\cdot 2^2=3\cdot 7\cdot 2^2=84.$$

最后我们再证明一个定理, 它指出 $\mathbf{F}_q$ 上不可约多项式 $f(x)$ 的周期怎样地决定了 $f(x^t)$ 的不可约因式的周期, 这里 t 是一个与 q 互素的素数.

定理 2 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个 n 次不可约多项式, $f(x)\neq x$, 而 $f(x)$ 的周期是 $p(f)$. 再设 t 是一个与 q 互素的素数. 如果 $t\mid p(f)$, 那么 $f(x^t)$ 的每一个不可约因式的周期都等于 $tp(f)$. 如果 $t\nmid p(f)$, 那么 $f(x^t)$ 有一个不可约因式的周期等于 $p(f)$, 而它其余的不可约因式的周期都等于 $tp(f)$.

证. 令 $g(x)=f(x^t)$. 那么

$$g'(x)=f'(x^t)\cdot tx^{t-1}.$$

因 $f(x)$ 不可约，于是 $f(x)$ 与 $f'(x)$ 互素，因此 $g(x)=f(x^t)$ 与 $f'(x^t)$ 互素．又因 $(t, q)=1$, 所以 $g(x)$ 也与 tx^{t-1} 互素．因此 $(g(x), g'(x))=1$．所以 $g(x)$ 没有重因式．假定 $g(x)$ 分解成 $\mathbf{F}_q$ 上不可约多项式 $f_1(x), f_2(x), \cdots, f_r(x)$ 之积

$$g(x)=\prod_{i=1}^{r} f_i(x).$$

那么 $f_1(x), f_2(x), \cdots, f_r(x)$ 两两相异．设 $\partial^0 f_i(x)=n_i$, 并假定 $f_i(x)$ 的周期是 $p(f_i)$.

令 $m=[n, n_1, n_2, \cdots, n_r]$. 根据第一章 §5 定理 6, $\mathbf{F}_{q^m}$ 有子域, $\mathbf{F}_{q^n}$, $\mathbf{F}_{q^{n_1}}$, $\mathbf{F}_{q^{n_2}}$, $\cdots$, $\mathbf{F}_{q^{n_r}}$. 因 $f(x)$ 的根都属于 $\mathbf{F}_{q^n}$, $f_i(x)$ 的根都属于 $\mathbf{F}_{q^{n_i}}(1\leqslant i\leqslant r)$, 所以 $f(x), f_1(x), f_2(x), \cdots, f_r(x)$ 的根都属于 $\mathbf{F}_{q^m}$.

设 ξ 是 $f_i(x)$ 在 $\mathbf{F}_{q^m}$ 中的一个根，即 $f_i(\xi)=0$, 那么 $g(\xi)=0$. 因此 $f(\xi^t)=0$. 于是 ξ^t 是个 $p(f)$ 阶元，即 $(\xi^t)^{p(f)}=1$. 因此 $\xi^{tp(f)}=1$. 那么根据第一章 §4 定理 4, $p(f_i)\mid tp(f)$. 首先注意

i) 如果 $t\mid p(f_i)$, 那么 ξ^t 就是个 $p(f_i)/t$ 阶元, 但已证 ξ^t 是个 $p(f)$ 阶元．所以 $p(f_i)/t=p(f)$. 因此 $p(f_i)=tp(f)$.

ii) 如果 $t\nmid p(f_i)$, 因 t 是素数，就有 $(t, p(f_i))=1$. 那么 ξ^t 和 ξ 有相同的阶．即 ξ^t 也是个 $p(f_i)$ 阶元．因此 $p(f_i)=p(f)$.

先设 $t\mid p(f)$. 这时不可能出现 $t\nmid p(f_i)$ 的情形；否则由 ii) 从 $t\nmid p(f_i)$ 推出 $p(f_i)=p(f)$, 这与 $t\mid p(f)$ 的假设相违．于是由 i) 从 $t\mid p(f_i)$ 推出 $p(f_i)=tp(f)$, 对 $i=1, 2, \cdots, r$.

再设 $t\nmid p(f)$. 于是 $(t, p(f))=1$. 那么有正整数 s 存在使 $ts\equiv 1(\bmod p(f))$. 设 η 是 $f(x)$ 的一个根．那么 $\eta, \eta^q, \eta^{q^2}, \cdots, \eta^{q^{n-1}}$ 就是 $f(x)$ 的全部根．我们有

$$g(\eta^s)=f(\eta^{st})=f(\eta)=0.$$

不妨假定 η^s 是 $f_1(x)$ 的一个根. 因 η^s 与 η 有相同的阶, 所以 $p(f_1)=p(f)$. 如果 $t\nmid p(f_i)$, 那么由 ii) 就有 $p(f_i)=p(f)$. 于是有 η^{s_i} 是 $f_i(x)$ 的根, 而 $(s_i, p(f))=1$. 从 $f_i(\eta^{s_i})=0$ 推出 $g(\eta^{s_i})=f(\eta^{s_it})=0$. 因此 $\eta^{s_it}=\eta^{q^j}$, $0\leqslant j\leqslant n-1$. 于是 $\eta^{s_i}=\eta^{sq^j}$. 但 η^{sq^j} 与 η^s 同时是 $f_1(x)$ 的根, 而 $g(x)$ 没有重因式, 所以 $f_i(x)=f_1(x)$. 因此对于 $i>1$, 一定有 $t|p(f_i)$. 那么根据 i) 就有 $p(f_i)=tp(f)$ 对 $i>1$.

这样定理 2 就完全证明了.

我们举一个例子来说明怎样运用定理 2 来计算一些多项式的周期.

例 3 假定已知 $f(x)=x^{84}+x^5+1$, $f(x^3)=x^{252}+x^{15}+1$, $f(x^9)=x^{756}+x^{45}+1$ 都是 $\mathbf{F}_2$ 上的不可约多项式. 并假定已知 $f(x)$ 的周期

$$p(f)=3^2\cdot7^2\cdot13\cdot29\cdot43\cdot113\cdot127\cdot337\cdot1429\cdot5419\cdot14449$$

试求 $f(x^3)$ 和 $f(x^9)$ 的周期.

我们知道 $(3, 2)=1$ 而 $3|p(f)$. 因此根据定理 2 可知, $f(x^3)$ 的周期

$$p(f(x^3))=3^3\cdot7^2\cdot13\cdot29\cdot43\cdot113\cdot127\cdot337\cdot1429\cdot5419\cdot14449$$

仍根据定理 2 可知,

$$p(f(x^9))=3^4\cdot7^2\cdot13\cdot29\cdot43\cdot113\cdot127\cdot337\cdot1429\cdot5419\cdot14449$$

§3 因式分解的一个方法

在 §2 中我们介绍了计算有限域 $\mathbf{F}_q$ 上一个零次项不等于 0 的多项式 $f(x)$ 的周期的一个方法; 根据这个方法, 需要先将 $f(x)$ 分解成 $\mathbf{F}_q$ 上不可约多项式的乘积. 在第四章 §3

中我们指出，确定一切码长 n 的 q 元循环码的问题，化为 $\mathbf{F}_q$ 上多项式 x^n-1 的因式分解问题. 因此讨论 $\mathbf{F}_q$ 上多项式的因式分解问题是有意义的.

设 $\mathbf{F}_q$ 是 q 个元素的有限域, q 是一个素数的幂. 设 $f(x)$ 是 $\mathbf{F}_q$ 上的一个多项式. 如果 $f(0)=0$, 那么 $x|f(x)$; 设 $x^k|f(x)$ 而 $x^{k+1}\nmid f(x)$, 那么可以写 $f(x)=x^kf_0(x)$, 而 $f_0(0)\neq 0$. 因此不妨设 $f(0)\neq 0$. 再设 $\partial^0 f(x)=n$. 我们知道, 如果 $f(x)$ 可约, $f(x)$ 一定有一个次数 $\leqslant n/2$ 的不可约因式 $g(x)$. 如果 $\partial^0 g(x)=m$, 那么根据第一章 § 5 引理 2 一定有 $g(x)|x^{q^m}-x$. 又因 $f(0)\neq 0$, 所以 $g(0)\neq 0$, 因此

$$g(x)\,|\,x^{q^m-1}-1.$$

这样一来，为了将 $f(x)$ 分解成不可约多项式的乘积，可先计算下面这些最高公因式

$$(f(x),\ x^{q^i-1}-1),\ i=1,\ 2,\ \cdots,\ [n/2],$$

其中 $[n/2]$ 表示不大于 $n/2$ 的最大的整数，如果这些最高公因式都等于 1，那么 $f(x)$ 在 $\mathbf{F}_q$ 上就一定不可约. 否则，求上面这些最高公因式的过程就有可能得到 $f(x)$ 的一个真因式 $f_1(x)$. 于是可以写 $f(x)=f_1(x)f_2(x)$. 再将上述方法施行到 $f_1(x)$, $f_2(x)$ 上去，如此继续下去，就有可能将 $f(x)$ 分解成不可约多项式的乘积. 当然如果 $f(x)$，或中间过程中得到的某一个因式，是一些两两相异的同次数的不可约多项式的乘积，这个方法就失效. 为此我们下面再介绍 Berlekamp 的一个方法*，利用它总可以将 $f(x)$ 分解成两两不同的不可约多项式的幂的乘积.

首先，我们注意，当 $f(x)$ 是 $\mathbf{F}_q$ 上的不可约多项式时，$\mathbf{F}_q[x]_{f(x)}$ 是域. 那么这时 $\mathbf{F}_q[X]$ 中的多项式

$$X^q-X \tag{1}$$

* 见[17]，第六章，§ 1.

在 $\mathbf{F}_q[x]_{f(x)}$ 中只有 q 个根,即 $\mathbf{F}_q$ 中的 q 个元素. 其次,再考察 $f(x)$ 是一个不可约多项式 $p_1(x)$ 的幂的情形,即

$$f(x)=p_1(x)^{e_1},\ e_1>0.$$

如果 $g(x)\in\mathbf{F}_q[x]_{f(x)}$ 是(1)的一个根,那么

$$g(x)^q-g(x)\equiv 0\pmod{f(x)}.$$

但

$$X^q-X=\prod_{s\in\mathbf{F}_q}(X-s),\tag{2}$$

上式右方是个连乘积,它的意思是:如果把 $\mathbf{F}_q$ 中的 q 个元素记作 $s_1,\ s_2,\ \cdots,\ s_q$,那么

$$\prod_{s\in\mathbf{F}_q}(X-s)=(X-s_1)(X-s_2)\cdots(X-s_q).$$

将 $g(x)$ 代入(2)式就有

$$\prod_{s\in\mathbf{F}_q}(g(x)-s)\equiv 0\pmod{f(x)},$$

即
$$f(x)\,\Big|\,\prod_{s\in\mathbf{F}_q}(g(x)-s).$$

我们先证明

引理 1 设 $g(x)$ 是 $\mathbf{F}_q$ 上的任一多项式,而 s_1 和 s_2 是 $\mathbf{F}_q$ 中两个不同的元素,那么

$$(g(x)-s_1,\ g(x)-s_2)=1.$$

证. 实际上,

$$\frac{-1}{s_1-s_2}(g(x)-s_1)+\frac{1}{s_1-s_2}(g(x)-s_2)=1.$$

因此 $g(x)-s_1$ 与 $g(x)-s_2$ 互素.

再回到上面的讨论,因 $f(x)$ 是一个不可约多项式 $p_1(x)$ 的幂,所以根据引理 1,我们有

$$f(x)\,|\,g(x)-s,\ \text{对某一个}\ s\in\mathbf{F}_q.$$

但 $g(x)\in\mathbf{F}_q[x]_{f(x)}$,即 $\partial^0 g(x)<\partial^0 f(x)$. 所以

$$g(x)=s\in\mathbf{F}_q.$$

这证明了,当 $f(x)$ 是一个不可约多项式的幂时,X^q-X 在

$\mathbf{F}_q[x]_{f(x)}$ 中仍只有 q 个根，即是 $\mathbf{F}_q$ 中的 q 个元素.

再考察一般情形. 设

$$f(x)=p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_r(x)^{e_r}, \tag{3}$$

其中 $p_1(x), p_2(x), \cdots, p_r(x)$ 是 $\mathbf{F}_q[x]$ 里的 r 个两两不同的不可约多项式，而 $e_1, e_2, \cdots, e_r$ 是 r 个正整数. 根据第一章 § 8 定理 4，我们有直和分解

$$\mathbf{F}_q[x]_{f(x)}=\mathbf{F}_q[x]'_{p_1(x)^{e_1}}\dot{\oplus}\mathbf{F}_q[x]'_{p_2(x)^{e_2}}\dot{\oplus}\cdots\dot{\oplus}\mathbf{F}_q[x]'_{p_r(x)^{e_r}} \tag{4}$$

其中 $\mathbf{F}_q[x]'_{p_i(x)^{e_i}}(i=1, 2, \cdots, r)$ 都是 $\mathbf{F}_q[x]_{f(x)}$ 的理想，而 $\mathbf{F}_q[x]'_{p_i(x)^{e_i}}$ 与 $\mathbf{F}_q[x]_{p_i(x)^{e_i}}$ 同构.

如果 $g(x)\,(\in\mathbf{F}_q[x]_{f(x)})$ 是多项式(1)的一个解，即在 $\mathbf{F}_q[x]_{f(x)}$ 中:

$$g(x)^q-g(x)=0.$$

我们回忆

$$g(x)^q=\underbrace{g(x)\odot g(x)\odot\cdots\odot g(x)}_{q\text{个}}$$

$$=(\underbrace{g(x)\cdot g(x)\cdot\cdots\cdot g(x)}_{q\text{个}})_{f(x)}.$$

根据环 $\mathbf{F}_q[x]_{f(x)}$ 的直和分解式，可以将 $g(x)$ 唯一地表成

$$g(x)=g_1(x)\oplus g_2(x)\oplus\cdots\oplus g_r(x),\quad g_i(x)\in\mathbf{F}_q[x]'_{p_i(x)^{e_i}}.$$

于是 $$g(x)^q=g_1(x)^q\oplus g_2(x)^q\oplus\cdots\oplus g_r(x)^q.$$

那么

$$0=g(x)^q-g(x)=(g_1(x)^q-g_1(x))$$
$$\oplus(g_2(x)^q-g_2(x))\oplus\cdots\oplus(g_r(x)^q-g_r(x)).$$

而 $$g_i(x)^q-g_i(x)\in\mathbf{F}_q[x]'_{p_i(x)^{e_i}}\quad i=1, 2, \cdots, r.$$

因(4)是直和分解，因此 0 只有一种表示法

$$0=\underbrace{0\oplus 0\oplus\cdots\oplus 0}_{r\text{个}}.$$

所以 $$g_i(x)^q-g_i(x)=0,\ i=1, 2, \cdots, r.$$

即 $g_1(x), g_2(x), \cdots, g_r(x)$ 都是(1)的解.

反之，如果 $g_1(x)$，$g_2(x)$，…，$g_r(x)$ 分别属于 $\mathbf{F}_q[x]'_{f_i(x)^{e_i}}$，而且都是(1)的解，那么显然

$$g(x)=g_1(x)\oplus g_2(x)\oplus\cdots\oplus g_r(x)$$

也是(1)的解.

这证明了，$\mathbf{F}_q[x]_{f(x)}$ 中(1)的解的个数等于各个

$$\mathbf{F}_q[x]'_{f_i(x)^{e_i}}\quad(i=1,\ 2,\ \cdots,\ r)$$

中(1)的解的个数之积，但是 $\mathbf{F}_q[x]'_{p_i(x)^{e_i}}$ 与 $\mathbf{F}_q[x]_{p_i(x)^{e_i}}$ $(i=1,\ 2,\ \cdots,\ r)$ 同构，而刚才已经证明了每个 $\mathbf{F}_q[x]_{p_i(x)^{e_i}}$ $(i=1,\ 2,\ \cdots,\ r)$ 中(1)的解的个数都等于 q. 因此 $\mathbf{F}_q[x]_{f(x)}$ 中(1)的解的个数等于 q^r. 我们证明了

定理 1 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个次数 $\geqslant 1$ 的多项式，那么多项式 X^q-X 在 $\mathbf{F}_q[x]_{f(x)}$ 中解的个数一定是 q 的一个幂. 更进一步，$f(x)$ 分解成 $\mathbf{F}_q[x]$ 中 r 个两两不同的不可约多项式的幂的乘积，当且仅当多项式 X^q-X 在 $\mathbf{F}_q[x]_{f(x)}$ 中解的个数是 q^r.

系理 $\mathbf{F}_q[x]$ 中的一个次数 $\geqslant 1$ 的多项式是 $\mathbf{F}_q[x]$ 中一个不可约多项式的幂，当且仅当多项式 X^q-X 在 $\mathbf{F}_q[x]_{f(x)}$ 中解的个数是 q.

仍设 $f(x)\in\mathbf{F}_q[x]$. 并设 $\partial^0 f(x)=n$. 我们知道，$\mathbf{F}_q[x]_{f(x)}$ 可以看作是 $\mathbf{F}_q$ 上的 n 维向量空间. 令 V 是多项式(1)在 $\mathbf{F}_q[x]_{f(x)}$ 中的解的全体所组成的集合，即

$$V=\{g(x)\mid\partial^0 g(x)<\partial^0 f(x)$$

而 $$g(x)^q-g(x)\equiv 0\ (\operatorname{mod} f(x))\}.$$

如果 $g_1(x)$，$g_2(x)\in V$，即

$$g_1(x)^q-g_1(x)\equiv 0\quad(\operatorname{mod} f(x)),$$
$$g_2(x)^q-g_2(x)\equiv 0\quad(\operatorname{mod} f(x)),$$

那么 $$(g_1(x)-g_2(x))^q=g_1(x)^q-g_2(x)^q$$
$$\equiv g_1(x)-g_2(x)\quad(\operatorname{mod} f(x)),$$

$$(sg_1(x))^q = s^q g_1(x)^q \equiv sg_1(x) \pmod{f(x)},$$

第二式中的 $s\in\mathbf{F}_q$. 因此 $g_1(x)-g_2(x)$, $sg_1(x)\in V$. 这证明了 V 是 $\mathbf{F}_q[x]_{f(x)}$ 的一个子空间. 这样一来，定理1可改述成

定理2 设 $f(x)\in\mathbf{F}_q[x]$ 而 $\partial^0 f(x)\geqslant 1$. 令

$$V=\{g(x)\mid \partial^0 g(x)<\partial^0 f(x)$$

而 $$g(x)^q-g(x)\equiv 0 \pmod{f(x)}\},$$

那么 $f(x)$ 分解成 r 个两两不同的不可约多项式的幂的乘积，当且仅当 V 是 $\mathbf{F}_q$ 上的 r 维向量空间.

系理 $f(x)$ 是 $\mathbf{F}_q[x]$ 中一个不可约多项式的幂，当且仅当 $\dim V=1$.

V 不仅可用来计算 $f(x)$ 分解成多少个两两不同的不可约多项式的幂的乘积，还可以用来得到 $f(x)$ 的分解式(3). 我们先证明

定理3 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中首项系数是1的多项式，而 $g(x)\in V$，那么

$$f(x)=\prod_{s\in\mathbf{F}_q}(f(x),\ g(x)-s). \tag{5}$$

更进一步，如果 $f(x)$ 有分解式

$$f(x)=p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_r(x)^{e_r},$$

其中 $p_1(x)$, $p_2(x)$, $\cdots$, $p_r(x)$ 是 $\mathbf{F}_q$ 上两两不同的不可约多项式，而 e_1, e_2, $\cdots$, e_r 都是正整数，那么对每个 $i=1, 2, \cdots, r$，都有唯一的一个 $s_i\in\mathbf{F}_q$ 使

$$p_i(x)^{e_i}\mid g(x)-s_i,\quad i=1, 2, \cdots, r.$$

而 $$p_i(x)^{e_i}\nmid g(x)-s,\ 若\ s\neq s_i.$$

证. 显然有

$$(f(x),\ g(x)-s)\mid f(x).$$

根据引理1，如 $s_1\neq s_2$，则

$$(g(x)-s_1,\ g(x)-s_2)=1.$$

于是 $$((f(x),\ g(x)-s_1),\ (f(x),\ g(x)-s_2))=1.$$

因此

$$\prod_{s\in\mathbf{F}_q}(f(x),\ g(x)-s)\mid f(x). \tag{6}$$

另一方面，因 $g(x)\in V$，即 $g(x)$ 适合(1)．我们知道(2)式总成立．将 $g(x)$ 代入(2)式中的 X，就有

$$\prod_{s\in\mathbf{F}_q}(g(x)-s)\equiv 0(\bmod f(x))$$

即

$$f(x)\Big|\prod_{s\in\mathbf{F}_q}(g(x)-s).$$

于是

$$p_i(x)^{e_i}\Big|\prod_{s\in\mathbf{F}_q}(g(x)-s),\ i=1,\ 2,\ \cdots,\ r.$$

根据引理1，连乘积中的 $g(x)-s(s\in\mathbf{F}_q)$ 两两互素．因此有唯一确定的一个 $s_i\in\mathbf{F}_q$ 使

$$p_i(x)^{e_i}\mid g(x)-s_i\quad i=1,\ 2,\ \cdots,\ r$$

而

$$p_i(x)^{e_i}\nmid g(x)-s,\ 若\ s\neq s_i.$$

于是

$$p_i(x)^{e_i}\mid(f(x),\ g(x)-s_i),\ i=1,\ 2,\ \cdots,\ r.$$

仍根据引理1，$s_1,\ s_2,\ \cdots,\ s_r$ 这 r 个元素一定两两相异．因此

$$f(x)\Big|\prod_{i=1}^{r}(f(x),\ g(x)-s_i) \tag{7}$$

那么从(6)，(7)两式就推出(5)式成立．定理3就证完了．

我们给出下面这个注记．如果 $g(x)$ 是 $\mathbf{F}_q$ 中的元素（注意 $\mathbf{F}_q$ 中的元素一定属于 V），那么分解式(5)退化：

$$\begin{aligned}f(x)&=\prod_{s\in\mathbf{F}_q}(f(x),\ g(x)-s)\\&=(f(x),\ 0)\prod_{s\in\mathbf{F}_q^*}(f(x),\ s)=f(x)\prod_{s\in\mathbf{F}_q^*}1.\end{aligned}$$

但是如果 $\partial^0 g(x)\geqslant 1$，分解式(5)就是一个真分解式，即 $f(x)$ 不可能作为一个因式出现在(5)式右方．

仍设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中首项系数是1的多项式，并设 $f(x)$ 有分解式(3)．再设

$$g_1(x)=1,\ g_2(x),\ g_3(x),\ \cdots,\ g_r(x)$$

是 V 的一组基，而

$$1\leqslant \partial^0 g_i(x)<\partial^0 f(x),\quad i=2,\ 3,\ \cdots,\ r,$$

那么对每对 $(i,\ j)$，$i,\ j=1,\ 2,\ \cdots,\ r$，根据定理 3 有唯一确定的一个元素 $s_{ij}\in\mathbf{F}_q$ 使

$$p_i(x)^{e_i}\,|\,g_j(x)-s_{ij},\quad i,\ j=1,\ 2,\ \cdots,\ r. \tag{8}$$

而

$$p_i(x)^{e_i}\,|\,g_j(x)-s,\ \text{若}\ s\neq s_{ij}, \tag{9}$$

我们得到 $\mathbf{F}_q$ 上的一个 $r\times r$ 矩阵

$$S=(s_{ij})_{1\leqslant i,j\leqslant r}.$$

我们证明

引理 2 S 是个非异矩阵.

证. 假定 S 的 r 个列有一线性关系

$$\sum_{j=1}^{r} c_j s_{ij}=0,\quad i=1,\ 2,\ \cdots,\ r,$$

其中 $c_1,\ c_2,\ \cdots,\ c_r\in\mathbf{F}_q$. 于是

$$p_i(x)^{e_i}\,\Big|\,\sum_{j=1}^{r} c_j g_j(x),\quad i=1,\ 2,\ \cdots,\ r.$$

那么

$$f(x)\,\Big|\,\sum_{j=1}^{r} c_j g_j(x).$$

但

$$\partial^0\left(\sum_{j=1}^{r} c_j g_j(x)\right)\leqslant \max(\partial^0 g_1(x),\ \partial^0 g_2(x),\ \cdots,\ \partial^0 g_r(x))$$
$$<\partial^0 f(x),$$

所以

$$\sum_{j=1}^{r} c_j g_j(x)=0.$$

但 $g_1(x),\ g_2(x),\ \cdots,\ g_r(x)$ 是 V 的一组基，因此一定有 $c_1=c_2=\cdots=c_r=0$. 这证明 S 的 r 个列一定线性无关. 因此 S 是非异矩阵.

从引理 2 可以推出

定理 4 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中一个首项系数是 1 的多项式，并假定 $f(x)$ 有分解式(3). 再设 $g_1(x)=1$, $g_2(x)$, $g_3(x)$, $\cdots$, $g_r(x)$ 是 V 的一组基，而 $1\leqslant\partial^0 g_i(x)<\partial^0 f(x)$，对 $i=2, 3, \cdots, r$. 假定 $s_{ij}(i, j=1, 2, \cdots, r)$ 是由 (i, j) 唯一确定的适合条件(8)和(9)的 $\mathbf{F}_q$ 中的元素，那么对任意一对 (i_1, i_2), $i_1\neq i_2$ 而 $1\leqslant i_1, i_2\leqslant r$，至少有一个 j 存在使 $s_{i_1j}\neq s_{i_2j}$. 因此

$$\left.\begin{array}{l} p_{i_1}^{e_{i_1}}(x)\mid g_j(x)-s_{i_1j},\ p_{i_1}^{e_{i_1}}(x)\nmid g_j(x)-s_{i_2j}, \\ p_{i_2}^{e_{i_2}}(x)\nmid g_j(x)-s_{i_1j},\ p_{i_2}^{e_{i_2}}(x)\mid g_j(x)-s_{i_2j}. \end{array}\right\}. \tag{10}$$

证. 根据引理 2, S 是非异矩阵，因此 S 的任意两行都不同. 那么对于 S 的第 i_1 行和第 i_2 行来说，至少有一个 j 存在使 $s_{i_1j}\neq s_{i_2j}$. 再由(8), (9)两式就推出(10)式成立.

下面我们介绍一个将 $\mathbf{F}_q[x]$ 中的多项式分解成不可约多项式的幂的乘积的方法. 上面证明的定理 2, 定理 3 和定理 4 是这个方法的理论根据.

设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个首项系数为 1 的 n 次多项式，而 $n\geqslant 1$. 要将 $f(x)$ 分解成不可约多项式的幂的乘积，可以按以下步骤进行:

1) 令

$$V=\{g(x)\mid\partial^0 g(x)<\partial^0 f(x)$$

而
$$g(x)^q\equiv g(x)\ (\bmod f(x))\},$$

并设 V 是 r 维的. 选出 V 的一组基来:

$$g_1(x)=1,\ g_2(x),\ g_3(x),\ \cdots,\ g_r(x),$$

其中
$$1\leqslant\partial^0 g_i(x)\leqslant\partial^0 f(x),\ i=2, 3, \cdots, r.$$

2) 用辗转相除法计算

$$(f(x),\ g_2(x)-s),\ s\in\mathbf{F}_q.$$

对每一个 s 都算完之后，根据定理 3, 我们有

$$f(x)=\prod_{s\in\mathbf{F}_q}(f(x),\ g_2(x)-s).$$

将 $f(x)$ 的上述分解式中等于 1 的那些因式略去，并改记

$$f(x)=f_{21}(x)f_{22}(x)\cdots f_{2r_2}(x). \tag{11}$$

3) 如果 $r_2=r$，那么根据定理 2，$f_{21}(x)$，$f_{22}(x)$，…，$f_{2r_2}(x)$ 就都是不可约多项式的幂．我们的目的已经达到，不必再计算下去了．如果 $r_2<r$，那么对每个 $j=1, 2, \cdots, r_2$ 和每个 $s\in\mathbf{F}_q$，用辗转相除法计算

$$(f_{2j}(x),\ g_3(x)-s).$$

因
$$g_3(x)^q-g_3(x)\equiv 0 \pmod{f(x)},$$
所以
$$g_3(x)^q-g_3(x)\equiv 0 \pmod{f_{2j}(x)}.$$
令
$$g_{3j}(x)=(g_3(x))_{f_{2j}(x)},$$
那么
$$g_{3j}(x)^q-g_{3j}(x)\equiv 0 \pmod{f_{2j}(x)}.$$
根据定理 3，我们有

$$f_{2j}(x)=\prod_{s\in\mathbf{F}_q}(f_{2j}(x),\ g_{3j}(x)-s),\quad j=1, 2, \cdots, r_2.$$

但显然

$$(f_{2j}(x),\ g_3(x)-s)=(f_{2j}(x),\ g_{3j}(x)-s),$$

因此

$$f_{2j}(x)=\prod_{s\in\mathbf{F}_q}(f_{2j}(x),\ g_3(x)-s),\quad j=1, 2, \cdots, r_2.$$

将 $f_{2j}(x)$ $(j=1, 2, \cdots, r_2)$ 的上述分解式中等于 1 的那些因式略去，再将它们代入(11)式，并改记成

$$f(x)=f_{31}(x)f_{32}(x)\cdots f_{3r_3}(x). \tag{12}$$

4) 如果 $r_3=r$，我们的目的已经达到，不必再算下去了．如果 $r_3<r$，那么对每个 $j=1, 2, \cdots, r_3$ 和每个 $s\in\mathbf{F}_q$，用辗转相除法计算

$$(f_{3j}(x),\ g_4(x)-s).$$

同理可得

$$f_{3j}(x)=\prod_{s\in\mathbf{F}_q}(f_{3j}(x),\ g_4(x)-s),\quad j=1, 2, , \cdots, r_3.$$

再将$f_{3j}(x)(j=1, 2, \cdots, r)$的上述分解式中等于1的那些因式略去，然后将它们代入(12)式，并改记成

$$f(x)=f_{41}(x)f_{42}(x)\cdots f_{4r_4}(x).$$

5) 如此继续下去．根据定理4，对任意一对(i_1, i_2)，$i_1\neq i_2$，$1\leqslant i_1, i_2\leqslant r$，总有一个$g_j(x)$使(10)式成立，这样$p_{i_1}(x)^{e_{i_1}}$和$p_{i_2}(x)^{e_{i_2}}$就分别出现在不同的两个$f_{jk}(x)$和$f_{jk'}(x)$中，这里$f_{jk}(x)$和$f_{jk'}(x)$是上述步骤重复$j-1$步时出现在$f(x)$的分解式

$$f(x)=f_{j1}(x)f_{j2}(x)\cdots f_{jr_j}(x)$$

中的两个因式．因此总存在一个$l\leqslant r$使$r_l=r$．这时

$$f(x)=f_{l1}(x)f_{l2}(x)\cdots f_{lr}(x)$$

就是$f(x)$分解成不可约多项式的幂的乘积的分解式．

上面介绍的因式分解方法的前提是要先求出V的一组基．如何求V的一组基，可以按照以下步骤进行：

1.1) 计算

$$(x^0)_{f(x)}=1,\ (x^q)_{f(x)},\ (x^{2q})_{f(x)},\ \cdots,\ (x^{(n-1)q})_{f(x)},$$

其中$n=\partial^0 f(x)$．和§2中完全一样，这些计算可以用移位寄存器来进行．设

$$(x^{jq})_{f(x)}=\sum_{i=0}^{n-1}a_{ij}x^i,\quad a_{ij}\in\mathbf{F}_q.$$

我们就得到一个$n\times n$矩阵

$$A=(a_{ij})_{0\leqslant i,j\leqslant n-1}.$$

我们把A的行(列)从上到下(从左到右)依序叫做第0行(列)，第1行(列)，第2行(列)，…，第$n-1$行(列)．

设
$$g(x)=\sum_{j=0}^{n-1}g_jx^j,$$

那么

$$g(x)^q = g(x^q) = \sum_{j=0}^{n-1} g_j x^{jq}$$

$$\equiv \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} g_j a_{ij} x^i \pmod{f(x)}.$$

于是

$$g(x)^q - g(x) \equiv \sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1} a_{ij} g_j - g_i\right) x^i \pmod{f(x)}.$$

因此 $g(x)\in V$，当且仅当

$$(A-I)(g_0, g_1, g_2, \cdots, g_{n-1})' = 0,$$

即当且仅当 $(g_0, g_1, g_2, \cdots, g_{n-1})$ 属于线性方程组

$$(A-I)(x_0, x_1, x_2, \cdots, x_{n-1})' = 0 \tag{13}$$

的解空间. 设 $\dim V = r$，那么 $A-I$ 的秩是 $n-r$.

附带地，由此即可推出下面的系理.

系理 $f(x)$ 是 $\mathbf{F}_q[x]$ 中的一个不可约多项式的幂，当且仅当 $A-I$ 的秩是 $n-1$.

1.2) 令 $B=A-I$. 将 B 经若干次行的初等变换化为阶梯形矩阵

$$B_0 = \begin{pmatrix} 0\cdots0 & 1 & *\cdots* & 0 & *\cdots* & 0 & *\cdots* & \cdots & 0 & *\cdots* \\ 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & 0 & *\cdots* & \cdots & 0 & *\cdots* \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & \cdots & 0 & *\cdots* \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & \cdots & 1 & *\cdots* \\ & & & & 0^{(r,n)} & & & & & \end{pmatrix}$$

第 i_0 列　　第 i_1 列　　第 i_2 列　　第 i_{n-r-1} 列

再经若干次行的初等变换，将 B_0 的第 0 行，第 1 行，第 2 行，…，第 $n-r-1$ 行分别变到第 i_0 行，第 i_1 行，第 i_2 行，…，第 i_{n-r-1} 行，B_0 就化成

$$
B_1=\left(\begin{array}{c|c|c|c|c|c}
0^{(i_0,i_0)} & 0 & 0 & 0 & \cdots & 0 \\
\hline
0 & \begin{array}{c} 1 \quad * \cdots * \\ 0^{(i_1-i_0-1,\, i_1-i_0)} \end{array} & \begin{array}{c} 0 \quad * \cdots * \\ 0 \end{array} & \begin{array}{c} 0 \quad * \cdots * \\ 0 \end{array} & \begin{array}{c} \cdots \\ \cdots \end{array} & \begin{array}{c} 0 \quad * \cdots * \\ 0 \end{array} \\
\hline
0 & 0 & \begin{array}{c} 1 \quad * \cdots * \\ 0^{(i_2-i_1-1,\, i_2-i_1)} \end{array} & \begin{array}{c} 0 \quad * \cdots * \\ 0 \end{array} & \begin{array}{c} \cdots \\ \cdots \end{array} & \begin{array}{c} 0 \quad * \cdots * \\ 0 \end{array} \\
\hline
0 & 0 & 0 & \begin{array}{c} 1 \quad * \cdots * \\ 0^{(i_3-i_2-1,\, i_3-i_2)} \end{array} & \begin{array}{c} \cdots \\ \cdots \end{array} & \begin{array}{c} 0 \quad * \cdots * \\ 0 \end{array} \\
\hline
0 & 0 & 0 & 0 & \ddots & \vdots \\
\hline
0 & 0 & 0 & 0 & \cdots & \begin{array}{c} 1 \quad * \cdots * \\ 0^{(n-i_{n-r-1}-1,\, n-i_{n-r-1})} \end{array}
\end{array}\right)
$$

注意 B_1 是所谓的三角幂等矩阵，即

i) B_1 的主对角线之下的元素都等于 0.

ii) 如果 B_1 的主对角线上有一个元素等于 0，那么这个 0 所在的行中的元素全都等于 0.

iii) 如果 B_1 的主对角线上有一个元素等于 1，那么这个 1 所在的列中其余的元素都等于 0.

iv) $B_1^2=B_1$.

1.3) 显然方程组

$$B_1(x_0, x_1, x_2, \cdots, x_{n-1})'=0 \tag{14}$$

与方程组(13)等价，因此它们的解空间相等.

从 $B_1^2=B_1$ 推出

$$B_1(I-B_1)=0.$$

容易看出来，$I-B_1$ 一共有 r 个非零列，而这 r 个非零列线性无关. 因此 $I-B_1$ 的秩是 r. 它的 r 个非零列就是方程组(14)(也是方程组(13))的解空间的一组基. 设

$$(b_{0j}, b_{1j}, b_{2j}, \cdots, b_{n-1j})' \quad j=1, 2, \cdots, r$$

是 $I-B_1$ 的 r 个非零列. 令

$$g_j(x)=\sum_{i=0}^{n-1} b_{ij}x^i, \quad j=1, 2, \cdots, r,$$

那么

$$g_1(x), g_2(x), \cdots, g_r(x)$$

就是 V 的一组基.

我们再指出，因 A 的第 0 列是将 $x^0=1$ 表成 $1, x, x^2, \cdots, x^{n-1}$ 的线性组合的系数组成的列，所以 A 的第 0 列是 $(1, 0, 0, \cdots, 0)'$. 于是 $B=A-I$ 的第 0 列的元素全都是 0. B 经若干次行的初等变换变成 B_1, B_1 的第 0 列的元素也全都是 0. 于是 $I-B_1$ 的第 0 列就是 $(1, 0, 0, \cdots, 0)$，它相应的多项式 $g_1(x)=1$.

第1.2)步是将B经若干次行的初等变换化为三角幂等矩阵B_1. 为了编程序的方便,我们介绍另一个将B直接化成B_1的方法. 这个方法是将下列四个步骤重复n次来达到目的.

i) 如果矩阵第$n-1$列(即最右边的一列)的元素都等于0, 或这一列最下边的元素(即$(n-1, n-1)$位置的元素)不等于0, 那就去进行ii). 如果矩阵第$n-1$列的元素不全等于0, 但$(n-1, n-1)$位置的元素等于0, 那就去找一个最靠右的等于0的对角线元素,设为(i, i)位置的元素, 而$(i, n-1)$位置的元素不等于0, 然后就将第i行与第$n-1$行(即第末行)对调,接着就去进行ii). 如果等于0的对角线元素所在的行的最右边的元素都等于0, 就去将第$n-1$列中最下面的一个非0元所在的行与第$n-1$行对调,接着去进行ii).

ii) 如果矩阵的$(n-1, n-1)$位置的元素等于0, 就去进行iv), 否则将矩阵第$n-1$行乘以它的$(n-1, n-1)$位置元素的逆.

iii) 将矩阵第$n-1$行乘以适当的元素加到其余各行去,使矩阵第$n-1$列中除最后一个元素外其余元素都等于0.

iv) 将矩阵的行向下作循环移位, 并将列向右作循环移位,如下面所示:

$$\begin{pmatrix} \text{第 } 0 \text{ 行} \\ \text{第 } 1 \text{ 行} \\ \text{第 } 2 \text{ 行} \\ \vdots \\ \text{第 } n-1 \text{ 行} \end{pmatrix} \to \begin{pmatrix} \text{第 } n-1 \text{ 行} \\ \text{第 } 0 \text{ 行} \\ \text{第 } 1 \text{ 行} \\ \vdots \\ \text{第 } n-2 \text{ 行} \end{pmatrix},$$

$$\begin{pmatrix} \text{第} & \text{第} & \text{第} & & \text{第} \\ 0 & 1 & 2 & \cdots & n-1 \\ \text{列} & \text{列} & \text{列} & & \text{列} \end{pmatrix} \to \begin{pmatrix} \text{第} & \text{第} & \text{第} & & \text{第} \\ n-1 & 0 & 1 & \cdots & n-2 \\ \text{列} & \text{列} & \text{列} & & \text{列} \end{pmatrix}.$$

注意，将上述算法重复 n 次，就将矩阵的各列向右作了 n 次循环移位，因此各列又回到原位，即等于没有对列进行变换.

把 $\mathbf{F}_q[x]$ 中一个次数 $\geqslant 1$ 的多项式 $f(x)$ 分解成一些因式的乘积，而且知道每个因式都是一个不可约多项式的幂以后，还需要把这些不可约多项式找出来并算出它们分别在那些因式中出现的次数. 为了解决这个问题，我们先证明

定理 5 设 $f(x)$ 是 $\mathbf{F}_q[x]$ 中一个首项系数等于 1 的不可约多项式的幂，并假定 $f'(x)\neq 0$. 如果 $(f(x), f'(x))=1$，那么 $f(x)$ 不可约. 如果 $(f(x), f'(x))\neq 1$，那么 $f(x)/(f(x), f'(x))$ 不可约. 令

$$p(x)=f(x)/(f(x), f'(x)),$$

那么

$$f(x)=p(x)^e,$$

其中

$$e=\partial^0 f(x)/\partial^0 p(x).$$

证. 设

$$f(x)=p(x)^e.$$

$p(x)$ 是 $\mathbf{F}_q[x]$ 中首项系数等于 1 的不可约多项式，而

$$e=\partial^0 f(x)/\partial^0 p(x),$$

那么

$$f'(x)=ep(x)^{e-1}p'(x).$$

因 $f'(x)\neq 0$，所以

$$(f(x), f'(x))=p(x)^{e-1}.$$

如果 $(f(x), f'(x))=1$，那么 $e=1$，这时 $f(x)=p(x)$ 不可约. 如果 $(f(x), f'(x))\neq 1$，那么

$$p(x)=f(x)/(f(x), f'(x)).$$

因此 $f(x)/(f(x), f'(x))$ 不可约. 这证明了定理 5.

基于定理 5，如果已知 $\mathbf{F}_q[x]$ 中次数 $\geqslant 1$ 的首项系数等于 1 的多项式 $f(x)$ 是某个不可约多项式的幂，那么可以按照以下步骤将这个不可约多项式求出来：

1) 设 q 是素数 p 的幂，那么 $\mathbf{F}_q$ 的特征是 p. 根据第一章 §3 定理 5 及其系理，可将 $f(x)$ 的系数不等于 0 的各项的

x 的幂次的公因数 p^m 提出来，得到

$$f(x)=h(x)^{p^m},$$

使得 $h(x)$ 至少有一个系数不等于 0 的项的 x 的幂次不被 p 除尽. 这时一定有 $h'(x)\neq 0$.

2) 计算 $$(h(x),\ h'(x)).$$

如果 $(h(x),\ h'(x))=1$, 那么 $h(x)$ 不可约. 如果 $(h(x),\ h'(x))\neq 1$, 令

$$p(x)=h(x)/(h(x),\ h'(x)),$$

那么 $h(x)=p(x)^e$, $e=\partial^0 h(x)/\partial^0 p(x)$. 于是

$$f(x)=p(x)^{ep^m}.$$

本节介绍的因式分解的方法是可以编成程序在电子计算机上进行计算的.

我们举两个例子来阐明上面介绍的因式分解的算法.

例 1 将 $\mathbf{F}_2$ 的多项式

$$f(x)=x^9+x+1$$

分解成不可约多项式的乘积.

先计算

$$(x^0)_{f(x)},\ (x^2)_{f(x)},\ (x^4)_{f(x)},\ \cdots,\ (x^{16})_{f(x)},$$

从而得到矩阵 A

$$A=\begin{pmatrix}1&0&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0&0\\0&1&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0&0\\0&0&1&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&1&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0&1\end{pmatrix},$$

那么 $$B=A-I=\begin{pmatrix}0&0&0&0&0&0&0&0&0\\0&1&0&0&0&1&0&0&0\\0&1&1&0&0&1&0&0&0\\0&0&0&1&0&0&1&0&0\\0&0&1&0&1&0&1&0&0\\0&0&0&0&0&1&0&1&0\\0&0&0&1&0&0&1&1&0\\0&0&0&0&0&0&0&1&1\\0&0&0&0&1&0&0&0&0\end{pmatrix}.$$

用行的初等变换将 B 化成阶梯形矩阵

$$B_0=\begin{pmatrix}0&1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0&0\\0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&0\end{pmatrix},$$

再将 B_0 的行互换，将 B_0 化成三角幂等矩阵

$$B_1=\begin{pmatrix}0&0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0&0\\0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\end{pmatrix}.$$

容易看出 $I-B_1$ 只有一个非零列，因此 $f(x)$ 一定是某一个不可约多项式的幂.

再计算 $$f'(x)=x^8+1.$$

显然有 $$1\cdot f(x)+x\cdot f'(x)=1$$

因此 $$(f(x),\ f'(x))=1.$$

于是 $f(x)$ 是 $\mathbf{F}_2$ 上的不可约多项式.

例 2 将 $\mathbf{F}_2$ 上的多项式

$$f(x)=x^8+x^4+x^3+x^2+x+1$$

分解成不可约多项式的乘积.

先计算

$$(x^0)_{f(x)},\ (x^2)_{f(x)},\ (x^4)_{f(x)},\ \cdots,\ (x^{14})_{f(x)}.$$

从而得到矩阵

$$A=\begin{pmatrix}1&0&0&0&1&0&1&1\\0&0&0&0&1&0&1&0\\0&1&0&0&1&1&1&1\\0&0&0&0&1&1&1&1\\0&0&1&0&1&1&0&1\\0&0&0&0&0&1&1&0\\0&0&0&1&0&1&1&0\\0&0&0&0&0&0&1&1\end{pmatrix},$$

那么 $$B=A-I=\begin{pmatrix}0&0&0&0&1&0&1&1\\0&1&0&0&1&0&1&0\\0&1&1&0&1&1&1&1\\0&0&0&1&1&1&1&1\\0&0&1&0&0&1&0&1\\0&0&0&0&0&0&1&0\\0&0&0&1&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}.$$

用行的初等变换将B化成阶梯形矩阵

$$B_0=\begin{pmatrix}0&1&0&0&0&0&0&1\\0&0&1&0&0&1&0&1\\0&0&0&1&0&1&0&0\\0&0&0&0&1&0&0&1\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{pmatrix},$$

再将B_0的行互换，将B_0化成三角幂等矩阵

$$B_1=\begin{pmatrix}0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&1\\0&0&1&0&0&1&0&1\\0&0&0&1&0&1&0&0\\0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0\end{pmatrix}.$$

那么
$$I-B_1=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&1&0&1\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1\end{pmatrix}.$$

$I-B_1$一共有3个非零列．由这3个非零列得出

$$g_1(x)=1,\ g_2(x)=x^5+x^3+x^2,$$
$$g_3(x)=x^7+x^4+x^2+x.$$

用辗转相除法计算 $f(x)$ 与 $g_2(x)$ 的最高公因式，得到

$$(f(x),\ g_2(x))=x^3+x+1.$$

再计算 $f(x)$ 与 $g_2(x)+1$ 的最高公因式，得到

$$(f(x),\ g_2(x)+1)=x^5+x^3+x^2+1.$$

于是 $$f(x)=(x^5+x^3+x^2+1)(x^3+x+1).$$

计算 $x^5+x^3+x^2+1$ 与 $g_3(x)$ 的最高公因式，得到

$$(x^5+x^3+x^2+1,\ g_3(x))=x^3+x^2+x+1.$$

再计算 $x^5+x^3+x^2+1$ 与 $g_3(x)+1$ 的最高公因式，得到

$$(x^5+x^3+x^2+1,\ g_3(x)+1)=x^2+x+1.$$

因此 $$f(x)=(x^3+x^2+x+1)(x^2+x+1)(x^3+x+1).$$

显然 x^2+x+1 和 x^3+x+1 都是 $\mathbf{F}_2$ 上的不可约多项式．令

$$f_1(x)=x^3+x^2+x+1.$$

那么 $$f_1'(x)=x^2+1=(x+1)^2.$$

于是 $$(f_1(x),\ f_1'(x))=(x+1)^2,$$
$$p_1(x)=f_1(x)/(f_1(x),\ f_1'(x))=x+1.$$

因此 $$f_1(x)=(x+1)^3.$$

所以 $$f(x)=(x+1)^3(x^2+x+1)(x^3+x+1).$$

§4　多项式 x^n-1 的因式分解

设 $\mathbf{F}_q$ 是 q 个元素的有限域，而 q 是一个素数 p 的幂．再设 n 是一个与 p 互素的正整数．我们来研究怎样把多项式

$$f(x)=x^n-1$$

在 $\mathbf{F}_q[x]$ 中分解成不可约多项式的乘积这个问题．

首先，我们注意，因 $(n,\ p)=1$，所以

$$f'(x)=nx^{n-1}\neq 0.$$

因此
$$(f(x),\ f'(x))=1.$$

由此推出 $f(x)$ 没有重因式. 这就是

定理 1 设 $\mathbf{F}_q$ 是 q 个元素的有限域, n 是与 q 互素的一个正整数, 那么 x^n-1 没有重因式.

其次, 因为 $(n,\ p)=1$, 所以 $(n,\ q)=1$. 那么 $q\in\mathbf{Z}_n^*$. 设 q 在 $\mathbf{Z}_n^*$ 中的阶是 m, 那么

$$q^m\equiv 1(\bmod n).$$

于是
$$n\mid q^m-1.$$

设 ξ 是 $\mathbf{F}_{q^m}$ 的一个本原元. 根据第一章 § 4 定理 4,

$$\alpha=\xi^{(q^m-1)/n}$$

就是 $\mathbf{F}_{q^m}^*$ 中的一个 n 阶元素, 我们把 α 叫做一个 n 次本原单位根. 这时

$$\alpha^0=1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{n-1}$$

这 n 个元素两两相异, 而且就是多项式 x^n-1 的全部 n 个根.

设 $f_1(x)$ 是 x^n-1 的一个首项系数等于 1 的不可约因式, 那么它的根必定是 α 的某些个幂. 假定 α^i 是 $f_1(x)$ 的一个根, 即

$$f_1(\alpha^i)=0,$$

那么
$$[f_1(\alpha^i)]^q=f_1(\alpha^{iq})=0,$$

即 α^{iq} 也是 $f_1(x)$ 的根. 设 l 是最小非负整数使

$$\alpha^{iq^l}=\alpha^i.$$

那么易证

$$\alpha^i,\ \alpha^{iq},\ \alpha^{iq^2},\ \cdots,\ \alpha^{iq^{l-1}} \tag{1}$$

两两相异, 而它们都是 $f_1(x)$ 的根. 令

$$h_1(x)=(x-\alpha^i)(x-\alpha^{iq})(x-\alpha^{iq^2})\cdots(x-\alpha^{iq^{l-1}}).$$

仿照第一章 § 5 定理 7 中相应的证明, 可证

$$h_1(x)\in\mathbf{F}_q[x].$$

但显然 $h_1(x) | f_1(x)$，而 $f_1(x)$ 不可约．所以

$$h_1(x) = f_1(x).$$

这证明了，(1)中 l 个 α 的幂就是 $f_1(x)$ 的全部的根．

反过来，设 $0 \leqslant i \leqslant n-1$．如果 l 是最小非负整数使

$$\alpha^{iq^l} = \alpha^i,$$

那么(1)中 l 个 α 的幂两两相异．令

$$h_1(x) = (x-\alpha^i)(x-\alpha^{iq})(x-\alpha^{iq^2})\cdots(x-\alpha^{iq^{l-1}}),$$

那么和刚才的道理一样，

$$h_1(x) \in \mathbf{F}_q[x].$$

设 $f_1(x)$ 是 $h_1(x)$ 的一个首项系数等于 1 的不可约因式．假定 $\alpha^{iq^j}(0 \leqslant j \leqslant l-1)$ 是 $f_1(x)$ 的一个根，那么和刚才一样可以证明 $\alpha^{iq^{j+1}}, \cdots, \alpha^{iq^{l-1}}, \alpha^{iq^l} = \alpha^i, \alpha^{iq}, \cdots, \alpha^{iq^{j-1}}$ 都是 $f_1(x)$ 的根．因此

$$f_1(x) = h_1(x).$$

这证明了，$h_1(x)$ 是 x^n-1 在 $\mathbf{F}_q[x]$ 中的不可约因式．

我们先给出下面这个定义．

定义 1 设 $a_0, a_1, a_2, \cdots, a_{l-1}$ 是从 0 到 $n-1$ 中选出来的 l 个两两相异的数．假定它们有性质：

$$a_i q \equiv a_{i+1} (\bmod n), \quad i = 0, 1, 2, \cdots, l-2,$$
$$a_{l-1} q \equiv a_0 (\bmod n).$$

我们就说它们组成 mod n 的一个 q 轮换，记作

$$(a_0, a_1, a_2, \cdots, a_{l-1}),$$

并把 l 叫做这个 q 轮换的长．

有了这个定义，我们可以把刚才得到的结论叙述成

定理 2 设 $\mathbf{F}_q$ 是 q 个元素的有限域，n 是与 q 互素的一个正整数．假定 α 是一个 n 次本原单位根(如果 q 在 $\mathbf{Z}_n^*$ 中的阶是 m，那么 $\mathbf{F}_{q^m}$ 中就一定有 n 次本原单位根)．设

$$f(x) = x^n - 1,$$

并设 $f_1(x)$ 是 $f(x)$ 的一个首项系数等于 1 的不可约因式，那么 $f_1(x)$ 的根都是 α 的一些幂 α^i, $0\leqslant i<n$, 而这些幂次组成 mod n 的一个 q 轮换. 反过来，如果 $(a_0, a_1, a_2, \cdots, a_{l-1})$ 是 mod n 的一个 q 轮换，那么

$$f_1(x)=(x-\alpha^{a_0})(x-\alpha^{a_1})(x-\alpha^{a_2})\cdots(x-\alpha^{a_{l-1}})$$

就是 x^n-1 的一个不可约因式.

系理 设 $\mathbf{F}_q$ 是 q 个元素的有限域，n 是与 q 互素的一个正整数，那么 x^n-1 在 $\mathbf{F}_q[x]$ 中分解成不可约因式的个数就等于 0, 1, 2, $\cdots$, $n-1$ 这 n 个数所分成的 mod n 的 q 轮换的个数.

根据上一节介绍的因式分解的方法，要将 x^n-1 分解成不可约因式的乘积，首先就要求出 V 的一组基，而

$$V=\{g(x)\mid\partial^0 g(x)<n$$

而 $$g(x)^q\equiv g(x)\bmod x^n-1\}.$$

上一节介绍的求 V 的基的方法是要算矩阵. 现在我们介绍一个简单的方法，当然这个方法是只对 x^n-1 适用的. 设 $(a_0, a_1, a_2, \cdots, a_{l-1})$ 是 mod n 的一个 q 轮换，令

$$\theta(x)=x^{a_0}+x^{a_1}+x^{a_2}+\cdots+x^{a_{l-1}}.$$

显然 $$\theta(x)^q\equiv\theta(x)\pmod{x^n-1},$$

假定 0, 1, 2, $\cdots$, $n-1$ 这 n 个数分成了 r 个 mod n 的 q 轮换. 对于每个 q 轮换，我们都得到 V 中的一个元素. 这样一共得到 V 的 r 个元素: $\theta_1(x)$, $\theta_2(x)$, $\cdots$, $\theta_r(x)$. 显然 x 的每个幂 $x^i(0\leqslant i\leqslant n-1)$ 在一个而且仅一个 $\theta_j(x)\,(1\leqslant j\leqslant r)$ 中出现. 因此 $\theta_1(x)$, $\theta_2(x)$, $\cdots$, $\theta_r(x)$ 在 $\mathbf{F}_q$ 上线性无关. 根据 §2 定理 2, V 在 $\mathbf{F}_q$ 上的维数等于 x^n-1 的不可约因式的个数; 根据上面定理 2 的系理，后者又等于 0, 1, 2, $\cdots$, $n-1$ 这 n 个数所分成的 mod n 的 q 轮换的个数. 这证明了 $\theta_1(x)$, $\theta_2(x)$, $\cdots$, $\theta_r(x)$ 是 V 的一组基. V 的一组基既已得到，利用

辗转相除法就可以将 x^n-1 分解成不可约多项式的乘积.

我们再指出，当 $q=2$ 时，V 实际上就是 $\mathbf{F}_2[x]_{x^n-1}$ 中幂等元的全体所组成的向量空间. 根据第一章§8定理7和定理8，要将 x^n-1 分解成不可约多项式的乘积，只要将1分解成 $\mathbf{F}_2[x]_{x^n-1}$ 中两两正交的本原幂等元的和就行了. 我们介绍一个如何从 V 的一组基 $\theta_1, \theta_2, \cdots, \theta_r$ 出发，将1分解成 $\mathbf{F}_2[x]_{x^n-1}$ 中 r 个两两正交的幂等元 $e_1, e_2, \cdots, e_r$ 的和的一个算法. 我们先证明

引理1 设 n 是奇数，V 是 $\mathbf{F}_2[x]_{x^n-1}$ 中幂等元的全体所组成的 $\mathbf{F}_2$ 上的向量空间，而 $\theta_1, \theta_2, \cdots, \theta_r$ 是 V 的一组基. 假定 $\mathbf{F}_2[x]_{x^n-1}$ 中的单位元素1分解成 t 个两两正交的幂等元 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_t$ 的和:

$$1=\varepsilon_1 \oplus \varepsilon_2 \oplus \cdots \oplus \varepsilon_t. \tag{2}$$

如果 $t<r$，那么总有一个 $\theta_i(1\leqslant i\leqslant r)$ 和一个 $\varepsilon_j(1=j\leqslant t)$ 使

$$\theta_i \odot \varepsilon_j \neq 0, \quad (1\oplus\theta_i)\odot \varepsilon_j \neq 0$$

同时成立.

证. 设有 $\theta_i(1\leqslant i\leqslant r)$ 使

$$\theta_i\odot\varepsilon_j=0 \text{ 或 } (1\oplus\theta_i)\odot\varepsilon_j=0, \quad \text{对 } j=1, 2, \cdots, t,$$

即
$$\theta_i\odot\varepsilon_j=0 \text{ 或 } \theta_i\odot\varepsilon_j=\varepsilon_j, \text{ 对 } j=1, 2, \cdots, t.$$

将(2)式双方同时乘以 θ_i，得出 θ_i 是某几个 $\varepsilon_j(j=1, 2, \cdots, t)$ 的和. 如果对每个 $\theta_i(1\leqslant i\leqslant r)$ 均有

$$\theta_i\odot\varepsilon_j=0 \text{ 或 } (1\oplus\theta_i)\odot\varepsilon_j=0, \text{ 对 } j=1, 2, \cdots, t,$$

那么 $\theta_1, \theta_2, \cdots, \theta_r$ 都是某几个 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_t$ 的和，即 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_t$ 的系数属于 $\mathbf{F}_2$ 的线性组合. 因 $r>t$，所以 $\theta_1, \theta_2, \cdots, \theta_r$ 就在 $\mathbf{F}_2$ 上线性相关. 这与 $\theta_1, \theta_2, \cdots, \theta_r$ 是 V 的一组基相矛盾. 因此一定有一个 θ_i 和一个 ε_j 使

$$\theta_i\odot\varepsilon_j\neq 0, \quad (1\oplus\theta_i)\odot\varepsilon_j\neq 0$$

同时成立.

我们可以把从 V 的一组基 $\theta_1, \theta_2, \cdots, \theta_r$ 出发，得出将 1 分解成 r 个两两正交的非零幂等元 $e_1, e_2, \cdots, e_r$ 的和的算法叙述如下：

"首先，将 1 分解成两个互相正交的幂等元 θ_1 和 $1\oplus\theta_1$ 的和：

$$1=\theta_1\oplus(1\oplus\theta_1).$$

如果 $r=2$，我们的目的已经达到．否则，将 θ_1 改记成 ε_1，将 $1\oplus\theta_1$ 改记成 ε_2:

$$1=\varepsilon_1\oplus\varepsilon_2.$$

根据引理 1，有一个 θ_i 和一个 ε_j，设为 ε_1，使

$$\theta_i\odot\varepsilon_1\neq 0, \quad (1\oplus\theta_i)\odot\varepsilon_1\neq 0.$$

那么
$$1=\theta_i\odot\varepsilon_1\oplus(1\oplus\theta_i)\odot\varepsilon_1\oplus\varepsilon_2,$$

而 $\theta_i\odot\varepsilon_1$, $(1\oplus\theta_i)\odot\varepsilon_1$ 和 ε_2 是 3 个两两正交的非 0 幂等元．

如果 $r=3$，我们的目的已经达到．否则继续用上面的方法进行下去，直到将 1 分成 r 个两两正交的非零幂等元的和．"

一旦将 $\mathbf{F}_2[x]_{x^n-1}$ 中的单位元素 1 分解成 r 个两两正交的非零幂等元 $e_1, e_2, \cdots, e_r$ 的和，这里 r 是 V 在 $\mathbf{F}_2$ 上的维数，$e_1, e_2, \cdots, e_r$ 一定是本原幂等元．令

$$f_i(x)=(x^n-1,\ 1-e_i), \quad i=1, 2, \cdots, r.$$

那么
$$x^n-1=f_1(x)f_2(x)\cdots f_r(x),$$

而 $f_1(x), f_2(x), \cdots, f_r(x)$ 是两两不同的不可约多项式．

当然上述算法是可以编出程序来在电子计算机上算的．当 n 不太大时，用手算也并无很大困难．

我们举一个例子来阐明上面的算法．

例 将 $\mathbf{F}_2$ 上的多项式

$$x^{15}-1$$

分解成不可约多项式的乘积．

先将0, 1, 2, …, 14这15个数分成mod 15的2轮换:
(1, 2, 4, 8), (3, 6, 12, 9), (5, 10), (7, 14, 13, 11), (0)
于是我们得到$\mathbf{F}_2[x]_{x^{15}-1}$中的5个幂等元

$$\theta_1=x+x^2+x^4+x^8,\ \theta_2=x^3+x^6+x^9+x^{12},$$

$$\theta_3=x^5+x^{10},\ \theta_4=x^7+x^{11}+x^{13}+x^{14},\ \theta_5=1.$$

它们组成$\mathbf{F}_2[x]_{x^{15}-1}$中所有幂等元所组成的向量空间$V$的一组基.

现在利用它们将1表成5个两两正交的非零幂等元的和.

首先,我们有

$$1=\theta_1\oplus(1\oplus\theta_1).$$

注意,

$$\theta_2\odot(1\oplus\theta_1)=\theta_1\oplus\theta_2\neq 0,$$

$$(1\oplus\theta_2)\odot(1\oplus\theta_1)=1\oplus\theta_2\neq 0,$$

因此有

$$1=\theta_1\oplus(\theta_1\oplus\theta_2)\oplus(1\oplus\theta_2),$$

而θ_1, $\theta_1\oplus\theta_2$和$1\oplus\theta_2$是三个两两正交的幂等元.

又有

$$\theta_3\odot\theta_1=\theta_2\oplus\theta_4\neq 0,$$

$$(1\oplus\theta_3)\odot\theta_1=\theta_1\oplus\theta_2\oplus\theta_4\neq 0,$$

$$\theta_3\odot(1+\theta_2)=\theta_1\oplus\theta_3\oplus\theta_4\neq 0,$$

$$(1\oplus\theta_3)\odot(1\oplus\theta_2)=\theta_1\oplus\theta_2\oplus\theta_3\oplus\theta_4\oplus\theta_5\neq 0.$$

因此

$$1=(\theta_2\oplus\theta_4)\oplus(\theta_1\oplus\theta_2\oplus\theta_4)\oplus(\theta_1\oplus\theta_2)$$
$$\oplus(\theta_1\oplus\theta_3\oplus\theta_4)\oplus(\theta_1\oplus\theta_2\oplus\theta_3\oplus\theta_4\oplus\theta_5)$$

就是将1分成5个两两正交的非零幂等元的和的分解. 令

$$e_1=\theta_2\oplus\theta_4,\quad e_2=\theta_1\oplus\theta_2\oplus\theta_4,\quad e_3=\theta_1\oplus\theta_2,$$

$$e_4=\theta_1\oplus\theta_3\oplus\theta_4,\quad e_5=\theta_1\oplus\theta_2\oplus\theta_3\oplus\theta_4\oplus\theta_5,$$

那么e_1, e_2, e_3, e_4, e_5都是本原幂等元.

$$
\begin{aligned}
e_1&= \quad x^3 \quad +x^6+x^7 \quad +x^9 \quad +x^{11}+x^{12}+x^{13}+x^{14},\\
e_2&= x+x^2+x^3+x^4 \quad +x^6+x^7+x^8+x^9 \quad +x^{11}+x^{12}+x^{13}+x^{14},\\
e_3&= x+x^2+x^3+x^4 \quad +x^6 \quad +x^8+x^9 \quad +x^{12};\\
e_4&= x+x^2 \quad +x^4+x^5 \quad +x^7+x^8 \quad +x^{10}+x^{11} \quad +x^{13}+x^{14},\\
e_5&=1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}.
\end{aligned}
$$

用辗转相除法可以算出

$$
\begin{aligned}
f_1(x)&=(x^{15}-1,\ 1-e_1)=x^4+x^3+1,\\
f_2(x)&=(x^{15}-1,\ 1-e_2)=x^4+x^3+x^2+x+1,\\
f_3(x)&=(x^{15}-1,\ 1-e_3)=x^4+x+1,\\
f_4(x)&=(x^{15}-1,\ 1-e_4)=x^2+x+1,\\
f_5(x)&=(x^{15}-1,\ 1-e_5)=x+1.
\end{aligned}
$$

于是

$$
\begin{aligned}
x^{15}-1=&(x^4+x^3+1)(x^4+x^3+x^2+x+1)\\
&\cdot(x^4+x+1)(x^2+x+1)(x+1).
\end{aligned}
$$

§5 确定不可约多项式和本原多项式的问题

在第一章§5中我们曾经指出，要具体造出p^n个元素的有限域$\mathbf{F}_{p^n}$(这里p是一个素数，而n是个正整数)，需要求出$\mathbf{F}_p$上一个n次不可约多项式. 在第三章§3中我们又指出，为了得到周期等于q^n-1的m序列，需要求出$\mathbf{F}_q$上一个n次本原多项式. 因此确定有限域$\mathbf{F}_p$(或$\mathbf{F}_q$)上的不可约多项式和本原多项式是有意义的. 因为$\mathbf{F}_q$上的n次本原多项式是周期等于q^n-1的n次不可约多项式，所以要确定n次本原多项式可以先确定n次不可约多项式，然后再计算一下它的周期是不是等于q^n-1. 关于后一个问题，即计算不可约多项式的周期这个问题，可以用§2中所介绍的方法来计算，但困难之点是当n和q适当大时，q^n-1的素因数分解问题.

至于怎样确定$\mathbf{F}_q$上的不可约多项式呢？我们知道不可

约多项式在多项式中的地位相当于素数在整数中的地位．在附录二里我们介绍了求素数的筛法．当然也可以用筛法来求不可约多项式．譬如将次数 $\geqslant 1$ 而 $\leqslant n$ 的多项式按次数排列成表，次数小的排在前面，次数大的排在后面，次数相等的多项式按某种规定排列先后．那么排在最前面的多项式就是不可约的，把它圈出来，再把它的倍式从表中划去．剩下的没有圈和没有划的多项式中排在最前面的多项式就是不可约的，把它圈出来，再把它的倍式从表中划去；等等．但这种做法，只要 n 适当大，工作量就太大．因此通常我们并不采用这种办法．

为了确定有限域上的不可约多项式，人们探讨了判定一个多项式是否可约的一些方法．利用这些方法去判定一个多项式是否可约．这样就可以从次数 $\leqslant n$ 的多项式的表中删去这些多项式，于是就得到了所有次数 $\leqslant n$ 的不可约多项式．§3 中介绍的方法就可以用来判定一个多项式是否可约，但这个方法毕竟比较复杂．因此人们先用一些简单的容易判定一个多项式是可约多项式的方法先删去一些可约多项式．然后再对剩下的多项式采用 §3 中介绍的方法来判定它究竟可约还是不可约．有时如果能够比较容易地找到 $\mathbf{F}_q[x]_{f(x)}$ 中一个 $\neq 1$ 的非零幂等元，那么根据第一章 §8 定理 7 也可以判定 $f(x)$ 可约．

常用的判定 $\mathbf{F}_2$ 上的一个 $n(\geqslant 1)$ 次多项式是可约多项式的方法有

1) 如果 $f(x)$ 的零次项等于 0，除非 $f(x)=x$，否则 $f(x)$ 一定可约．

2) 如果 $f(x)$ 中系数等于 1 的项的个数是偶数，那么 $f(x)$ 一定可约．

3) 如果 $f(x)$ 中系数等于 1 的项的 x 的幂次都是 2 的倍

数，那么 $f(x)$ 一定可约.

4) 如果$(f(x), f'(x))\neq 1$，那么 $f(x)$ 一定可约.

5) 如果 $f(x+1)$ 可约，那么 $f(x)$ 也可约.

6) 如果 $x^n f\left(\frac{1}{x}\right)$ 可约，那么 $f(x)$ 也可约，等等.

对于 $\mathbf{F}_2$ 上的三项式 $f_{n,k}(x)=x^n+x^k+1$(n, k 不同时是偶数)，还有

1) 设 $n\geqslant 4$. 当 $n\equiv 1 \pmod 3$ 而 $k\equiv 2 \pmod 3$ 或当 $n\equiv 2 \pmod 3$ 而 $k\equiv 1 \pmod 3$ 时，$f_{n,k}(x)$ 被 x^2+x+1 除尽，因此这时 $f_{n,k}(x)$ 可约.

2)* $f_{n,k}(x)$ 有偶数个不可约因式，当且仅当以下三情况之一成立:

i) n 是偶数，k 是奇数，$n\neq 2k$，而 $\frac{nk}{2}\equiv 0$ 或 $1 \pmod 4$.

ii) n 是奇数，k 是偶数，$k\nmid 2n$，而 $n\equiv \pm 3 \pmod 8$.

iii) n 是奇数，k 是偶数，$k\mid 2n$，而 $n\equiv \pm 1 \pmod 8$.

因此上述三情形之一成立时，$f_{n,k}(x)$ 一定可约.

Zierler, N. 和 Brillhart, J.** 利用上述这些判定 $\mathbf{F}_2$ 上的多项式和三项式可约的条件以及 § 3 介绍的方法，用计算机定出了 $\mathbf{F}_2$ 上所有次数 $\leqslant 1000$ 的不可约三项式，并对于已知 2^n-1 的素因数分解的那些 $n(\leqslant 1000)$ 次不可约三项式算出了它们的周期，因而定出了一些本原三项式. 他们的结果表明，并不是有任意次数的不可约三项式(和本原三项式). 但是任给一正整数 N，是否有次数 $\geqslant N$ 的本原三项式则不清楚.

当然如果已经知道一个 n 次本原多项式，可以用第三章 § 4 中介绍的方法去求其余的 n 次本原多项式.

---

* 见 Swan, R. G., Factorization of Polynomials over Finite Fields, *Pacific J. Math.*, **12** (1962), 1099—1106.

** On Primitive Trinomials, I, II; *Information and Control*, **13** (1968), 541—554; **14** (1969), 566—569.

附录一 集合和映射

集合和映射是近代数学中的两个基本概念. 我们在下面对它们作一扼要的介绍.

所谓集合就是指作为整体来考察的一堆东西. 例如, 有理数的全体就组成一个集合, 实数的全体也组成一个集合, 而 $\mathbf{Z}_p$ 是由 p 个元素 $0, 1, 2, \cdots, p-1$ 组成的集合. 组成集合的成员叫做这个集合的*元素*. 我们用

$$a \in M$$

表示 a 是集合 M 的元素, 读作 a 属于 M. 用

$$a \notin M$$

表示 a 不是集合 M 的元素, 读作 a 不属于 M.

所谓给了一个集合就是规定了这个集合是由哪些元素组成的. 通常有两种办法给出一个集合, 一种是列举出它的全部元素来, 一种是给出这个集合的元素所具有的特征性质, 譬如, $\mathbf{Z}_p$ 是由 $0, 1, 2, \cdots, p-1$ 这 p 个元素组成的集合, 记作

$$\mathbf{Z}_p = \{0, 1, 2, \cdots, p-1\},$$

这就是列举出 $\mathbf{Z}_p$ 的全部元素. 又如 $\mathbf{Q}[\sqrt{2}]$ 是由一切形状是

$$a + b\sqrt{2},$$

其中 a 和 b 是有理数, 的实数组成的集合, 记作

$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\},$$

这就是给出 $\mathbf{Q}[\sqrt{2}]$ 中元素的特征性质. 括号 $\{\cdots\}$ 中的符号 $|$ 之前的 $a+b\sqrt{2}$ 表明 $\mathbf{Q}[\sqrt{2}]$ 中元素的形状, 但 a, b

究竟是什么则由符号 | 之后的性质 $a, b\in\mathbf{Q}$ 所说明.

为了处理问题的方便，我们引进空集合的概念，我们把空集合看作是不包含任何元素的集合. 其余的集合则叫做非空集合，因此非空集合就是确包含元素的集合.

如果一个集合 M 所含的元素个数有限，我们就说 M 是有限集合，简称有限集，并用 $|M|$ 来代表 M 所含的元素个数. 我们把空集合看作是含 0 个元素的有限集. 如果 M 不是有限集，M 就叫无限集.

如果两个集合 M 与 N 含有完全相同的元素，即 $a\in M$，当且仅当 $a\in N$，那么就说它们相等，记作

$$M=N.$$

如果集合 M 的元素全是集合 N 的元素，即从 $a\in M$ 可以推出 $a\in N$，那么就说 M 是 N 的子集合，简称子集，记作

$$M\subset N \text{ 或 } N\supset M.$$

譬如，$\mathbf{Q}\subset\mathbf{R}$，$\mathbf{R}\subset\mathbf{C}$，而当 $p(x)$ 是 $\mathbf{Z}_p[x]$ 中的一个不可约多项式时，还有 $\mathbf{Z}_p\subset\mathbf{Z}_p[x]_{p(x)}$. 根据定义，每个集合都是它自己的子集合. 我们还规定，空集合是任一集合的子集合.

设 M 是一个集合，而 N 是 M 的一个子集合. 我们用 $M\setminus N$ 代表由 M 中不属于 N 的那些元素所组成的集合，即

$$M\setminus N=\{a\,|\,a\in M \text{ 而 } a\notin N\}.$$

换句话说，$M\setminus N$ 就是从 M 中除去属于 N 的那些元素以后，剩下的元素所组成的集合，例如，当 M 是全体整数组成的集合，而 N 是全体偶数(包括 0)组成的集合时，$M\supset N$ 而 $M\setminus N$ 就是由全体奇数组成的集合.

设 M 和 N 是两个集合. 既属于 M 又属于 N 的全体元素所组成的集合叫做 M 和 N 的交，记作

$$M\cap N.$$

即

$$M\cap N=\{a\,|\,a\in M \text{ 而且 } a\in N\}.$$

例如，当 M 是全体偶数组成的集合，而 N 是全体小于 7 的正整数所组成的集合时，

$$M\cap N=\{2,\ 4,\ 6\}.$$

显然有 $$M\cap N\subset M,\ M\cap N\subset N.$$

仍设 M 和 N 是两个集合. 属于集合 M 或者属于集合 N 的全体元素所组成的集合叫做 M 和 N 的并，记作

$$M\cup N.$$

例如 $$\{1,\ 2,\ 3,\ 4\}\cup\{2,\ 4,\ 5\}=\{1,\ 2,\ 3,\ 4,\ 5\}.$$

显然有 $$M\cup N\supset M,\ M\cup N\supset N.$$

集合的交和并这两个概念可以推广到任意多个(有限多个或无限多个)集合的情形去. 设 I 是一个足码集合. 设对于每个 $\alpha\in I$，都有一个集合 M_α，那么属于每一个 $M_\alpha(\alpha\in I)$ 的元素的全体组成的集合就叫做这些 M_α 的交，记作

$$\bigcap_{\alpha\in I}M_\alpha.$$

同样，属于任何一个 $M_\alpha(\alpha\in I)$ 的元素的全体组成的集合叫做这些 M_α 的并，记作

$$\bigcup_{\alpha\in I}M_\alpha.$$

显然有 $$\bigcap_{\alpha\in I}M_\alpha\subset M_\alpha,$$

$$\bigcup_{\alpha\in I}M_\alpha\supset M_\alpha.$$

下面再介绍映射的概念.

设 M 和 M' 是两个集合. 所谓从集合 M 到集合 M' 的一个映射，是指一个规则，它使 M 中每一个元素 a 都有 M' 中一个确定的元素 a' 与它对应. 设 σ 是从 M 到 M' 的一个映射，我们就记

$$\sigma:\ M\to M'.$$

如果 σ 使元素 $a'\in M'$ 与元素 $a\in M$ 对应，就记作

$$\sigma: a \to a',$$

有时也记作 $\sigma: (a) = a'$.

我们把 a' 叫做 a 在映射 σ 之下的象，而 a 叫做 a' 在映射 σ 之下的一个原象．我们有时也把从 M 到 M' 的一个映射叫做定义在 M 上而在 M' 中取值的一个函数．

设 σ 是从集合 M 到集合 M' 的一个映射，我们用

$$\sigma(M)$$

代表 M 在映射 σ 之下的象的全体，即

$$\sigma(M) = \{\sigma(a) \mid a \in M\}.$$

显然 $\sigma(M) \subset M'$.

如果 $\sigma(M) = M'$，映射 σ 就叫做是映上的．如果在映射 σ 之下，M 中不同的元素的象也一定不同，即由 $a_1 \neq a_2$ 一定有 $\sigma(a_1) \neq \sigma(a_2)$，我们就说 σ 是一对一的．一对一的而且映上的映射叫做一一对应．

设 M 是一个集合，将 M 的每个元素都映到它自身的映射

$$a \to a, \quad a \in M,$$

叫做集合 M 的恒同映射，记作 1_M，在不致引起混淆时，也可以简单地记作 1．显然，恒同映射是一一对应．

我们举几个例子来说明上面的概念．

例 1 $M = \{1, 2, 3, 4\}$，$M' = \{1', 2', 3'\}$．定义 $\sigma(1) = \sigma(2) = 1'$，$\sigma(3) = \sigma(4) = 3'$．映射 σ 不是映上的，因为 $2'$ 没有原象．σ 也不是一对一的，因为 1 和 2 的象相同，3 和 4 的象也相同．

例 2 $M = \mathbf{Z}$，而 M' 是全体非负整数的集合．定义从 M 到 M' 的一个映射 σ:

$$\sigma(a) = |a|, \quad a \in M.$$

那么 σ 是映上，但不是一对一的．

例 3 设 M 是全体正整数的集合，而

$$M'=\{x,\ x^2,\ x^3,\ \cdots\}$$

即 M' 是 x 的全体正幂次的集合. 定义从 M 到 M' 的一个映射

$$\sigma(n)=x^n,\ n\in M.$$

那么 σ 是映上的而且是一对一的，因而是一一对应。

附录二　整数的分解

用 $\mathbf{Z}$ 表示全体整数(正、负整数和 0)的集合. 我们知道在 $\mathbf{Z}$ 中定义了加法运算和乘法运算，而 $\mathbf{Z}$ 对于这两种运算是自封的. 我们也知道域的定义(见第一章 §1 定义 1)中的运算规则 I.1, I.2, I.3, I.4, II.1, II.2, II.3 和 III 在 $\mathbf{Z}$ 中都成立，而 II.4 在 $\mathbf{Z}$ 中却不成立. 因此 $\mathbf{Z}$ 不是域.

我们先来复习一下 $\mathbf{Z}$ 中的带余除法. 设 a 和 b 是两个整数，而 $b\neq 0$. 假定用 b 去除 a 所得的商是 q 而余数是 r. 那么可以写

$$a=qb+r,\ \ 0\leqslant r<|b|, \tag{1}$$

式中 $|b|$ 表示 b 的绝对值，这就是 $\mathbf{Z}$ 中的带余除法，而(1)式叫带余除法算式. 大家都知道，满足(1)式的整数 q 和 r 由 a 和 b 唯一决定，因此可以记

$$r=(a)_b,$$

并说 r 是 b 去除 a 所得的余数. 当 $r=0$ 时，我们就说 b 是 a 的因数，或 a 是 b 的倍数，也说 a 被 b 所整除，或 b 除得尽 a，并用符号

$$b\mid a$$

来表示. 我们还用符号 $b\nmid a$ 表示 b 除不尽 a. 显然，如果 b 是 a 的因数，而 $a\neq 0$，那么有

$$|b|<|a|.$$

设 a, b, c 都是整数，而 $c\neq 0$. 如果 c 既是 a 的因数，又是 b 的因数，我们就说 c 是 a 和 b 的公因数. 当 a 和 b 不全等于 0 时，a 和 b 的公因数中就有一个最大的；我们把 a 和 b 的

公因数中最大的那一个叫做 a 和 b 的最大公倍数，并用符号

$$(a,\ b)$$

来表示．当 a 和 b 都等于 0 时，那么任何一个整数都是它们的公因数，这时 a 和 b 没有最大公因数，因此符号(0, 0)没有意义．

设 a 和 b 都是不等于 0 的整数．我们来复习一下求 (a, b) 的辗转相除法，假定 $|a|>|b|$．根据带余除法算式，依次有

$$a=q_1b+r_1,\quad 0<r_1<|b|, \tag{2.1}$$

$$b=q_2r_1+r_2,\quad 0<r_2<r_1, \tag{2.2}$$

$$r_1=q_3r_2+r_3,\quad 0<r_3<r_2, \tag{2.3}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{n-3}=q_{n-1}r_{n-2}+r_{n-1},\quad 0<r_{n-1}<r_{n-2} \tag{2.n-1}$$

$$r_{n-2}=q_nr_{n-1}+r_n,\quad 0<r_n<r_{n-1} \tag{2.n}$$

$$r_{n-1}=q_{n+1}r_n. \tag{2.n+1}$$

那么
$$(a,\ b)=r_n.$$

实际上，由(2.n+1)式知 $r_n|r_{n-1}$，再由(2.n)式知 $r_n|r_{n-2}$，再由(2.n−1)式知 $r_n|r_{n-3}$，…，如此继续下去，最后由 $r_n|r_1$ 和 $r_n|b$ 及(2.1)式知 $r_n|a$．因此 r_n 是 a 和 b 的公因数．反过来，设 d 是 a 和 b 的一个公因数，即 $d|a$, $d|b$．那么由(2.1)式知 $d|r_1$，再由(2.2)式知 $d|r_2$，再由(2.3)式知 $d|r_3$，…，如此继续下去，最后由 $d|r_{n-2}$ 和 $d|r_{n-1}$ 及(2.n)式知 $d|r_n$．因此 $r_n=(a,\ b)$．

更进一步，可将(2.1)—(2.n)式改写成

$$r_1=1\cdot a+(-q_1)\cdot b, \tag{3.1}$$

$$r_2=1\cdot b+(-q_2)\cdot r_1, \tag{3.2}$$

$$r_3=1\cdot r_1+(-q_3)r_2, \tag{3.3}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{n-1}=1\cdot r_{n-3}+(-q_{n-1})\cdot r_{n-2}, \tag{3.n-1}$$

$$r_n=1\cdot r_{n-2}+(-q_n)\cdot r_{n-1}, \tag{3.n}$$

$(3.n)$式是说 r_n 是 r_{n-2} 和 r_{n-1} 的整数系数的线性组合. 将$(3.n-1)$式代入$(3.n)$式得

$$r_n=(-q_n)\cdot r_{n-3}+(1+q_nq_{n-1})\cdot r_{n-2}$$

这就是说 r_n 是 r_{n-3} 和 r_{n-2} 的整数系数的线性组合. 如此继续下去,就可以将 a 和 b 的最大公因数 r_n 表成 a 和 b 的整数系数的线性组合,即

$$r_n=ca+db,$$

其中 c 和 d 都是整数. 那么从上面这个式子立刻推出 a 和 b 的任一公因数都是 r_n 的因数.

我们举一个实例来说明怎样利用辗转相除法来求两个整数的最大公因数,并将它表成这两个整数的整系数线性组合. 设 $a=49$, $b=36$. 利用带余除法,依次得到下面的一系列算式

$$\begin{aligned}49&=1\cdot 36+13, \quad &13<36,\\36&=2\cdot 13+10, \quad &10<13,\\13&=1\cdot 10+3, \quad &3<10,\\10&=3\cdot 3+1, \quad &1<3,\\3&=3\cdot 1.\end{aligned}$$

这表明 $$(49,\ 36)=1.$$

将前四个式子改写成

$$\begin{aligned}13&=49-1\cdot 36,\\10&=36-2\cdot 13,\\3&=13-1\cdot 10,\\1&=10-3\cdot 3.\end{aligned}$$

将第三式右方代入第四式中的后一个3,再将所得算式中的10用第二式右方代入,最后将所得算式中的13用第一式右方代入,得

$$
\begin{aligned}
1 &= 10-3\cdot(13-1\cdot10)=(-3)\cdot13+4\cdot10 \\
&= (-3)\cdot13+4\cdot(36-2\cdot13) \\
&= 4\cdot36+(-11)\cdot13 \\
&= 4\cdot36+(-11)\cdot(49-1\cdot36) \\
&= (-11)\cdot49+15\cdot36,
\end{aligned}
$$

即
$$1=(-11)\cdot49+15\cdot36.$$

当 a 和 b 的最大公因数是 1 时，即当 $(a, b)=1$ 时，我们就说 a 和 b **互素**．例如，根据刚才的计算，我们知道 49 和 36 互素．当 a 和 b 互素时，即当 $(a, b)=1$ 时，根据上面的讨论可知，1 可以表成 a 和 b 的整系数的线性组合，即

$$1=ca+db,$$

其中 c 和 d 都是整数．

设 a 和 b 都是不等于 0 的整数．如果 c 既是 a 的倍数，又是 b 的倍数，我们就说 c 是 a 和 b 的**公倍数**．显然 $|ab|$ 是 a 和 b 的一个正的公倍数．因此 a 和 b 的正的公倍数中一定有一个最小的；我们把 a 和 b 的正的公倍数中最小的那一个叫做 a 和 b 的**最小公倍数**，并用符号

$$[a, b]$$

来表示．

显然对于任意有限多个不全等于 0 的整数 $a_1, a_2, \cdots, a_n$ 也可以定义它们的公因数和最大公因数，我们说 c 是它们的一个公因数，如果 c 是每一个 $a_i (i=1, 2, \cdots, n)$ 的因数；而它们的公因数中最大的那一个就叫它们的最大公因数；并用符号

$$(a_1, a_2, \cdots, a_n)$$

来表示．对于任意有限多个都不等于 0 的整数 $a_1, a_2, \cdots, a_n$ 也可以定义它们的公倍数和最小公倍数．我们说 b 是它们的一个公倍数，如果 b 是每一个 $a_i (i=1, 2, \cdots n)$ 的倍数；而它

们的正的公倍数中最小的那一个就叫它们的最小公倍数，并用符号

$$[a_1,\ a_2,\ \cdots,\ a_n]$$

来表示. 根据定义，显然有

$$\begin{aligned}(a_1,\ a_2,\ \cdots,\ a_n)&=(a_1,\ (a_2,\ \cdots,\ a_n))\\&=(a_1,\ (a_2,\ \cdots,\ (a_{n-1},\ a_n)\cdots)),\\ [a_1,\ a_2,\ \cdots,\ a_n]&=[a_1,\ [a_2,\ \cdots,\ a_n]]\\&=[a_1,\ [a_2,\ \cdots,\ [a_{n-1},\ a_n]\cdots]].\end{aligned}$$

设 p 是个大于 1 的整数. 我们说 p 是个素数如果 p 的正因数只有 1 和 p. 不是素数的大于 1 的整数就叫复合数. 我们知道素数的个数无限. 为了求出 ≤ 某一正数的所有的素数，可利用筛法. 譬如要求出 ≤100 的素数，可先将从 2 到 100 的整数依序列出：

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19
~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37
~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~
~~56~~ ~~57~~ ~~58~~ 59 ~~60~~ 61 ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73
~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ 79 ~~80~~ ~~81~~ ~~82~~ 83 ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~ ~~91~~
~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

2 是其中最小的一个数，2 就是一个素数，把 2 挑选出来，然后把 2 的倍数(不包括 2 本身在内)都划去. 剩下的没有划去的比 2 大的数里，3 是最小的一个数，3 就是一个素数，把 3 挑选出来，然后把剩下的数中 3 的倍数(不包括 3 本身在内)都划去. 如此继续下去，直到剩下的没有划去的也没有挑选出来的数里 11 是最小的一个数时为止. 因为 ≤100 的复合数一定有一个素因数 $\leqslant\sqrt{100}=10$，所以这时剩下的数就都是素数. 这样就得到了 ≤100 的素数表：

2 3 5 7 11 13 17 19 23 29 31 37 41
43 47 53 59 61 67 71 73 79 83 89 97

所谓的算术基本定理是下面的

定理1 大于1的整数都可以表成一些素数的乘积．如果不计这些素数在乘积中排列的先后次序，那么这种表法是唯一的．

证．设 n 是个大于1的整数．如果 n 是素数，n 自然是素数的乘积，即 $n=n$．如果 n 不是素数，那么 n 的大于1的因数中有一个最小的．设这个最小的是 p_1．因 p_1 的因数也是 n 的因数，所以 p_1 一定是素数．设

$$n=p_1n_1,\quad 1<n_1<n.$$

若 n_1 是素数，n 已表成素数之积．若 n_1 不是素数，令 p_2 是 n_1 的最小的大于1的因数，那么 p_2 一定是素数，设

$$n=p_1p_2n_2,\quad 1<n_2<n_1<n.$$

如此继续下去，得一串递减正整数

$$n>n_1>n_2>\cdots>1.$$

因此这样做下去不能超过 n 次．故最后必得

$$n=p_1p_2p_3\cdots p_r,$$

其中 $p_1, p_2, p_3, \cdots, p_r$ 都是素数．这证明了算术基本定理的第一部分．

为了证明第二部分，先证明下面这个引理．

引理1 设 p 是个素数而 $p|ab$，其中 a 和 b 都是整数，那么 $p|a$ 或 $p|b$．

证．如果 $p\nmid a$，那么 $(p, a)=1$．于是有整数 c 和 d 存在使

$$1=cp+da.$$

将上式双方都乘以 b，得

$$b=bc\cdot p+d\cdot ab$$

因 $p|ab$，所以 $p|b$．因此引理成立．

从引理1立刻推出：设 p 是素数而 $p|a_1a_2\cdots a_m$，那么

$p|a_1$, 或 $p|a_2$, …, 或 $p|a_m$.

现在来证明算术基本定理的第二部分. 设 n 是个大于 1 的整数, 并假定有两种方法把 n 表成素数的乘积:

$$n=p_1p_2\cdots p_r=q_1q_2\cdots q_s, \tag{4}$$

其中 p_1, p_2, …, p_r 和 q_1, q_2, …, q_s 都是素数. 我们对 r 用数学归纳法来证明表法的唯一性.

当 $r=1$ 时, $n=p_1$ 是素数. 因此 $s=1$; $n=p_1=q_1$, 这时表示法唯一.

现在假定对于任何大于 1 的整数, 如果它可以表成 $r-1$ 个素数的乘积, 那么表法一定唯一. 今证明将 n 表成素数之积的表法也唯一. 我们有 $p_1|n$, 即 $p_1|q_1q_2\cdots q_s$. 因此根据引理 1, $p_1|q_1$, 或 $p_1|q_2$, …, 或 $p_1|q_s$. 那么重新排列 q_1, q_2, …, q_s 之后, 可设 $p_1|q_1$. 因 p_1, q_1 都是素数, 所以 $p_1=q_1$. 那么从(4)式推出

$$p_2p_3\cdots p_r=q_2q_3\cdots q_s.$$

根据归纳法假设, 一定有 $r-1=s-1$ 而重排 q_2, q_3, …, q_s 之后一定有 $p_2=q_2$, $p_3=q_3$, …, $p_r=q_r$. 这证明了 n 表成素数的乘积的方法, 如不计这些素数在乘积中的先后次序, 是唯一的.

这样算术基本定理就完全证明了.

根据算术基本定理, 任何一个不等于 0 的整数 a 都可以表成下面的形状

$$a=\pm p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}, \tag{5}$$

其中 p_1, p_2, …, p_r 是两两不同的素数, e_1, e_2, …, e_r 是些正整数, 而"+"号或"−"号视 $a>0$ 或 $a<0$ 而定. (5)叫做 a 的*素因数分解式*.

假定 a, b, …, c 是有限多个不等于 0 的整数. 将它们表成

$$a=\pm p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m},$$
$$b=\pm p_1^{f_1}p_2^{f_2}\cdots p_m^{f_m},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$c=\pm p_1^{g_1}p_2^{g_2}\cdots p_m^{g_m},$$

其中 $p_1, p_2, \cdots, p_m$ 是两两不同的素数，而 $e_i, f_i, g_i(i=1, 2, \cdots, m)$ 都是 $\geqslant 0$ 的整数，那么 $a, b, \cdots, c$ 的最大公因数 $(a, b, \cdots, c)$ 和最小公倍数 $[a, b, \cdots, c]$ 分别是

$$(a, b, \cdots, c)=p_1^{\min(e_1,f_1,\cdots,g_1)}p_2^{\min(e_2,f_2,\cdots,g_2)}\cdots p_m^{\min(e_m,f_m,\cdots,g_m)}, \tag{6}$$

$$[a, b, \cdots, c]=p_1^{\max(e_1,f_1,\cdots,g_1)}p_2^{\max(e_2,f_2,\cdots,g_2)}\cdots p_m^{\max(e_m,f_m,\cdots,g_m)}, \tag{7}$$

其中 $\min(e_i, f_i, \cdots, g_i)$， $\max(e_i, f_i, \cdots, g_i)$

分别表示 $e_i, f_i, \cdots, g_i$ 中最小的一个数和最大的一个数．从上述最大公因数和最小公倍数的公式(6)和(7)立刻可以推出：对于任意两个正整数 a 和 b，总有

$$(a, b)\cdot[a, b]=a\cdot b.$$

附表一　2^n-1 的素因数分解表

($n \leqslant 100$)

n	2^n-1 的 素 因 数 分 解
1	1
2	3
3	7
4	$3\cdot5$
5	31
6	$3^2\cdot7$
7	127
8	$3\cdot5\cdot17$
9	$7\cdot73$
10	$3\cdot11\cdot31$
11	$23\cdot89$
12	$3^2\cdot5\cdot7\cdot13$
13	8191
14	$3\cdot43\cdot127$
15	$7\cdot31\cdot151$
16	$3\cdot5\cdot17\cdot257$
17	131071
18	$3^3\cdot7\cdot19\cdot73$
19	524287
20	$3\cdot5^2\cdot11\cdot31\cdot41$
21	$7^2\cdot127\cdot337$
22	$3\cdot23\cdot89\cdot683$
23	$47\cdot178481$
24	$3^2\cdot5\cdot7\cdot13\cdot17\cdot241$
25	$31\cdot601\cdot1801$
26	$3\cdot2731\cdot8191$
27	$7\cdot73\cdot262657$
28	$3\cdot5\cdot29\cdot43\cdot113\cdot127$

n	2^n-1 的素因数分解
29	233·1103·2089
30	3^2·7·11·31·151·331
31	2147483647
32	3·5·17·257·65537
33	7·23·89·599479
34	3·43691·131071
35	31·71·127·122921
36	3^3·5·7·13·19·37·73·109
37	223·616318177
38	3·174763·524287
39	7·79·8191·121369
40	3·5^2·11·17·31·41·61681
41	13367·164511353
42	3^2·7^2·43·127·337·5419
43	431·9719·2099863
44	3·5·23·89·397·683·2113
45	7·31·73·151·631·23311
46	3·47·178481·2796203
47	2351·4513·13264529
48	3^2·5·7·13·17·97·241·257·673
49	127·4432676798593
50	3·11·31·251·601·1801·4051
51	7·103·2143·11119·131071
52	3·5·53·157·1613·2731·8191
53	6361·69431·20394401
54	3^4·7·19·73·87211·262657
55	23·31·89·881·3191·201961
56	3·5·17·29·43·113·127·15790321
57	7·32377·524287·1212847
58	3·59·233·1103·2089·3033169
59	179951·3203431780337
60	3^2·5^2·7·11·13·31·41·61·151·331·1321

n	2^n-1 的素因数分解
61	2305843009213693951
62	$3\cdot715827883\cdot2147483647$
63	$7^2\cdot73\cdot127\cdot337\cdot92737\cdot649657$
64	$3\cdot5\cdot17\cdot257\cdot641\cdot65537\cdot6700417$
65	$31\cdot8191\cdot145295143558111$
66	$3^2\cdot7\cdot23\cdot67\cdot89\cdot683\cdot20857\cdot599479$
67	$193707721\cdot761838257287$
68	$3\cdot5\cdot137\cdot953\cdot26317\cdot43691\cdot131071$
69	$7\cdot47\cdot178481\cdot10052678938039$
70	$3\cdot11\cdot31\cdot43\cdot71\cdot127\cdot281\cdot86171\cdot122921$
71	$228479\cdot48544121\cdot212885833$
72	$3^3\cdot5\cdot7\cdot13\cdot17\cdot19\cdot37\cdot73\cdot109\cdot241\cdot433\cdot38737$
73	$439\cdot2298041\cdot9361973132609$
74	$3\cdot223\cdot1777\cdot25781083\cdot616318177$
75	$7\cdot31\cdot151\cdot601\cdot1801\cdot100801\cdot10567201$
76	$3\cdot5\cdot229\cdot457\cdot174763\cdot524287\cdot525313$
77	$23\cdot89\cdot127\cdot581283643249112959$
78	$3^2\cdot7\cdot79\cdot2731\cdot8191\cdot121369\cdot22366891$
79	$2687\cdot202029703\cdot1113491139767$
80	$3\cdot5^2\cdot11\cdot17\cdot31\cdot41\cdot257\cdot61681\cdot4278255361$
81	$7\cdot73\cdot2593\cdot71119\cdot262657\cdot97685839$
82	$3\cdot83\cdot13367\cdot164511353\cdot8831418697$
83	$167\cdot57912614113275649087721$
84	$3^2\cdot5\cdot7^2\cdot13\cdot29\cdot43\cdot113\cdot127\cdot337\cdot1429\cdot5419\cdot14449$
85	$31\cdot131071\cdot9520972806333758431$
86	$3\cdot431\cdot9719\cdot2099863\cdot2932031007403$
87	$7\cdot233\cdot1103\cdot2089\cdot4177\cdot9857737155463$
88	$3\cdot5\cdot17\cdot23\cdot89\cdot353\cdot397\cdot683\cdot2113\cdot2931542417$
89	618970019642690137449562111
90	$3^3\cdot7\cdot11\cdot19\cdot31\cdot73\cdot151\cdot331\cdot631\cdot23311\cdot18837001$
91	$127\cdot911\cdot8191\cdot112901153\cdot23140471537$
92	$3\cdot5\cdot47\cdot277\cdot1013\cdot1657\cdot30269\cdot178481\cdot2796203$

n	2^n-1 的素因数分解
93	7·2147483647·658812288653553079
94	3·283·2351·4513·13264529·165768537521
95	31·191·524287·420778751·30327152671
96	3^2·5·7·13·17·97·193·241·257·673·65537·22253377
97	11447·13842607235828485645766393
98	3·43·127·4363953127297·4432676798593
99	7·23·73·89·199·153649·599479·33057806959
100	3·5^3·11·31·41·101·251·601·1801·4051·8101·268501

附注: (1) 本表根据 'Kraitchik, M., On the Factorization of $2^n\pm1$, *Scripta Mathematica*, **18**(1952), 39—52 编成; $2^{95}-1$ 的素因数分解据 'Robinson, R. M., Some Factorizations of Numbers of the Form $2^n\pm1$, MTAC, **11** (1957), 265—268' 一文加以改正.

(2) 对于当 $n>100$ 时, 2^n-1 的素因数分解有兴趣的读者请参阅 'Rrillhart, J. and Selfridge, J. L., Some Factorizations of $2^n\pm1$ and Related Results, *Math. of Comp.*, **21** (1967), 87—96' 一文及该文所引文献.

附表二　F_2 上不可约多项式的表

（次数$\leqslant$10）

次数	不可约多项式	周期	次数	不可约多项式	周期
1	1 0		7	1 1 0 0 1 0 1 1	127
	1 1	1		1 1 1 0 1 1 1 1	127
2	1 1 1	3	8	1 0 0 0 1 1 0 1 1	51
3	1 0 1 1	7		1 0 0 0 1 1 1 0 1	255
4	1 0 0 1 1	15		1 0 0 1 0 1 0 1 1	255
	1 1 1 1 1	5		1 0 0 1 0 1 1 0 1	255
5	1 0 0 1 0 1	31		1 0 0 1 1 1 0 0 1	17
	1 0 1 1 1 1	31		1 0 0 1 1 1 1 1 1	85
	1 1 0 1 1 1	31		1 0 1 0 0 1 1 0 1	255
6	1 0 0 0 0 1 1	63		1 0 1 0 1 1 1 1 1	255
	1 0 0 1 0 0 1	9		1 0 1 1 0 0 0 1 1	255
	1 0 1 0 1 1 1	21		1 0 1 1 1 0 1 1 1	85
	1 0 1 1 0 1 1	63		1 0 1 1 1 1 0 1 1	85
	1 1 0 0 1 1 1	63		1 1 0 0 0 0 1 1 1	255
7	1 0 0 0 0 0 1 1	127		1 1 0 0 0 1 0 1 1	85
	1 0 0 0 1 0 0 1	127		1 1 0 0 1 1 1 1 1	51
	1 0 0 0 1 1 1 1	127		1 1 1 0 0 1 1 1 1	255
	1 0 0 1 1 1 0 1	127		1 1 1 0 1 0 1 1 1	17
	1 0 1 0 0 1 1 1	127	9	1 0 0 0 0 0 0 0 1 1	73
	1 0 1 0 1 0 1 1	127		1 0 0 0 0 1 0 0 0 1	511
	1 0 1 1 1 1 1 1	127		1 0 0 0 0 1 0 1 1 1	73

说明： (1) 不可约多项式栏中列出了不可约多项式各次幂的系数，最左侧是最高次幂的系数，然后依序是次高次幂的系数，…直到0次幂的系数。例如，111 代表多项式 x^2+x+1；100011011 代表多项式 $x^8+x^4+x^3+x+1$.

(2) 与表中不可约多项式互反的多项式未列入，例如，与 $x^8+x^4+x^3+x+1$ 互反的多项式 $x^8+x^7+x^5+x^4+1$ 就没有列入。

次数	不可约多项式	周期	次数	不可约多项式	周期
9	1 0 0 0 0 1 1 0 1 1	511	10	1 0 0 0 1 0 0 0 1 1 1	341
	1 0 0 0 1 0 1 1 0 1	511		1 0 0 0 1 0 1 0 0 1 1	341
	1 0 0 0 1 1 0 0 1 1	511		1 0 0 0 1 1 0 0 0 1 1	341
	1 0 0 1 0 0 1 0 1 1	73		1 0 0 0 1 1 0 0 1 0 1	1023
	1 0 0 1 0 1 1 0 0 1	511		1 0 0 0 1 1 0 1 1 1 1	1023
	1 0 0 1 0 1 1 1 1 1	511		1 0 0 1 0 0 0 1 0 1 1	1023
	1 0 0 1 1 0 0 1 0 1	73		1 0 0 1 0 0 1 1 0 0 1	341
	1 0 0 1 1 0 1 1 1 1	511		1 0 0 1 0 1 0 1 0 0 1	33
	1 0 0 1 1 1 0 1 1 1	511		1 0 0 1 0 1 0 1 1 1 1	341
	1 0 0 1 1 1 1 1 0 1	511		1 0 0 1 1 0 0 0 1 0 1	1023
	1 0 1 0 0 0 0 1 1 1	511		1 0 0 1 1 0 1 0 1 1 1	1023
	1 0 1 0 0 1 0 1 0 1	511		1 0 0 1 1 1 0 0 1 1 1	1023
	1 0 1 0 1 0 0 0 1 1	511		1 0 0 1 1 1 0 1 1 0 1	341
	1 0 1 0 1 0 1 1 1 1	511		1 0 0 1 1 1 1 0 0 1 1	1023
	1 0 1 0 1 1 0 1 1 1	511		1 0 0 1 1 1 1 1 1 1 1	1023
	1 0 1 0 1 1 1 1 0 1	511		1 0 1 0 0 0 0 1 0 1 1	93
	1 0 1 1 0 0 1 1 1 1	511		1 0 1 0 0 0 0 1 1 0 1	1023
	1 0 1 1 0 1 1 0 1 1	511		1 0 1 0 0 0 1 1 1 1 1	341
	1 1 0 0 0 1 0 0 1 1	511		1 0 1 0 0 1 0 0 0 1 1	1023
	1 1 0 0 0 1 1 1 1 1	511		1 0 1 0 0 1 1 1 1 0 1	1023
	1 1 0 0 1 1 1 0 1 1	511		1 0 1 0 1 0 0 0 0 1 1	1023
	1 1 0 1 0 0 1 1 1 1	511		1 0 1 0 1 0 1 0 1 1 1	1023
	1 1 0 1 0 1 1 0 1 1	511		1 0 1 0 1 1 0 0 1 1 1	341
	1 1 0 1 1 1 1 1 1 1	511		1 0 1 0 1 1 0 1 0 1 1	1023
	1 1 1 0 0 0 1 1 1 1	511		1 0 1 1 0 0 0 1 1 1 1	1023
10	1 0 0 0 0 0 0 1 0 0 1	1023		1 0 1 1 0 0 1 0 1 1 1	1023
	1 0 0 0 0 0 0 1 1 1 1	341		1 0 1 1 0 0 1 1 0 1 1	341
	1 0 0 0 0 0 1 1 0 1 1	1023		1 0 1 1 0 1 0 1 0 1 1	341
	1 0 0 0 0 0 1 1 1 0 1	341		1 0 1 1 1 0 0 0 1 1 1	1023
	1 0 0 0 0 1 0 0 1 1 1	1023		1 0 1 1 1 1 1 0 1 1 1	1023
	1 0 0 0 0 1 0 1 1 0 1	1023		1 0 1 1 1 1 1 1 0 1 1	1023
	1 0 0 0 0 1 1 0 1 0 1	93			

次数	不可约多项式	周期	次数	不可约多项式	周期
10	1 1 0 0 0 0 1 0 0 1 1	1023	10	1 1 0 1 0 1 1 1 1 1 1	341
	1 1 0 0 0 1 0 0 0 1 1	33		1 1 0 1 1 0 1 1 1 1 1	1023
	1 1 0 0 0 1 1 0 1 1 1	1023		1 1 0 1 1 1 1 0 1 1 1	341
	1 1 0 0 1 0 0 1 1 1 1	1023		1 1 1 0 0 0 0 1 1 1 1	341
	1 1 0 0 1 0 1 1 0 1 1	1023		1 1 1 0 0 0 1 0 1 1 1	1023
	1 1 0 0 1 1 1 1 1 1 1	1023		1 1 1 1 1 1 1 1 1 1 1	11
	1 1 0 1 0 1 0 0 1 1 1	93			

附注: 本表根据 'Marsh, R. W., Table of Irreducible Polynomials over GF (2) Through Degree 19, NSA, Washington, D. C., 1957' 编成。

附表三 F_2 上不可约三项式 x^n+x^k+1 的表

($2\leqslant n\leqslant 100$, $1\leqslant k\leqslant n/2$)

n	k	周 期 (或指数)	n	k	周 期 (或指数)
2	1	本原	15	4	本原
3	1	本原		7	本原
4	1	本原	17	3	本原
5	2	本原		5	本原
6	1	本原		6	本原
6	3	3^2	18	3	$3^3\cdot 7$
7	1	本原		7	本原
7	3	本原		9	3^3
9	1	73	20	3	本原
9	4	本原		5	$3\cdot 5^2$
10	3	本原	21	2	本原
11	2	本原		7	7^2
12	3	$3^2\cdot 5$	22	1	本原
	5	(5)	23	5	本原
14	5	(3)		9	本原
15	1	本原	25	3	本原

说明: (1) 因 x^n+x^k+1 和 $x^n+x^{n-k}+1$ 同时可约或不可约，而当它们不可约时，它们的周期相等，所以当 $n/2<k<n$ 时，三项式 x^n+x^k+1 是否不可约及是否本原可以从表中 $x^n+x^{n-k}+1$ 是否列入及是否本原来断定，而当 x^n+x^k+1 不可约时，它的周期等于表中 $x^n+x^{n-k}+1$ 的周期。

(2) 当 x^n+x^k+1 是本原多项式时，在表中周期(或指数)栏写明，当 x^n+x^k+1 是非本原的不可约三项式时，表中周期(或指数)栏中一般列出的是它的周期，但如周期较大，则列出指数。注意周期·指数 $=2^n-1$。周期(或指数)栏中，不加圆括号的数字是周期，加圆括号的数字是指数，如 x^6+x^3+1 的周期是 3^2，$x^{12}+x^5+1$ 的指数是 5。

附表三(续)

n	k	周　期　(或指数)	n	k	周　期　(或指数)
25	7	本原	49	12	本原
28	1	(3·5)		15	本原
	3	本原		22	本原
	9	本原	52	3	本原
	13	本原		7	(3)
29	2	本原		19	本原
30	1	(3^2·11)		21	本原
	9	3^2·11·31	54	9	3^4·7
31	3	本原		21	3^4·7·19·73
	6	本原	54	27	3^4
	7	本原	55	7	(23)
	13	本原		24	本原
33	10	(7)	57	4	(7)
	13	本原		7	本原
34	7	(3)		22	本原
35	2	本原		25	(7)
36	9	3^3·5	58	19	本原
	11	本原	60	1	本原
	15	3^3·7·13		9	3^2·5^2·11·31·41
39	4	本原		11	本原
	8	本原		15	3^2·5^2
	14	本原		17	(3·5·7·11)
41	3	本原		23	(5)
	20	本原	62	29	(3)
42	7	3^2·7^2	63	1	本原
44	5	(3·5)		5	本原
46	1	(3)		11	(7)
47	5	本原		28	7^2·73
	14	本原		31	本原
	20	本原	65	18	本原
	21	本原		32	本原
49	9	本原	66	3	3^2·23·89·683

n	k	周　期　(或指数)	n	k	周　期　(或指数)
68	9	本原	84	35	$3^2\cdot7^2\cdot13$
	33	本原		39	$3^2\cdot5\cdot29\cdot43\cdot113\cdot127$
71	6	本原	86	21	(3)
	9	本原	87	13	本原
	18	本原	89	38	本原
	20	本原	90	27	$3^3\cdot11\cdot31$
	35	本原	92	21	(5)
73	25	本原	93	2	本原
	28	本原	94	21	本原
	31	本原	95	11	本原
74	35	(3)		17	本原
76	21	(3)	97	6	本原
79	9	本原		12	本原
	19	本原		33	本原
81	4	本原		34	本原
	16	本原	98	11	本原
	35	本原		27	本原
84	5	(5)	100	15	$3\cdot5^3\cdot11\cdot31\cdot41$
	9	$3^2\cdot5\cdot29\cdot43\cdot113\cdot127$		19	(41)
	11	(5)		25	$3\cdot5^3$
	13	本原		37	本原
	27	$3^2\cdot5\cdot29\cdot43\cdot113\cdot127$		49	(11)

附注：本表根据 Zierler, N. and Brillhart, J., On Primitive Trinomials (mod 2), *Information and Coutrol* **13** (1968), 541—554 编成。

附表四　F_2 上本原多项式的表

（次数 ≤168，每个次数一个）

次数	本原多项式					次数	本原多项式				
1	1	0				23	23	5	0		
2	2	1	0			24	24	4	3	1	0
3	3	1	0			25	25	3	0		
4	4	1	0			26	26	8	7	1	0
5	5	2	0			27	27	8	7	1	0
6	6	1	0			28	28	3	0		
7	7	1	0			29	29	2	0		
8	8	6	5	1	0	30	30	16	15	1	0
9	9	4	0			31	31	3	0		
10	10	3	0			32	32	28	27	1	0
11	11	2	0			33	33	13	0		
12	12	7	4	3	0	34	34	15	14	1	0
13	13	4	3	1	0	35	35	2	0		
14	14	12	11	1	0	36	36	11	0		
15	15	1	0			37	37	12	10	2	0
16	16	5	3	2	0	38	38	6	5	1	0
17	17	3	0			39	39	4	0		
18	18	7	0			40	40	21	19	2	0
19	19	6	5	1	0	41	41	3	0		
20	20	3	0			42	42	23	22	1	0
21	21	2	0			43	43	6	5	1	0
22	22	1	0			44	44	27	26	1	0

说明：(1) 本原多项式栏中列出的是该多项式非零系数的幂次。例如，210 代表 x^2+x+1，86510 代表 $x^8+x^6+x^5+x+1$。

(2) 对于一个给定的次数 $n\leqslant 168$，如果有本原 n 次三项式存在，这个表里就列出一个本原三项式 x^n+x^k+1 而 k 尽可能地小；如果没有本原 n 次三项式存在，这个表里就列出了一个本原五项式 $x^n+x^{b+a}+x^b+x^a+1$，而 $0<a<b<n-a$，同时 a 尽可能地小，而在 a 尽可能小的前提下，b 又尽可能地小。参看第三章§10，例5。

附表四(续)

次数	本原多项式	次数	本原多项式
45	45 4 3 1 0	77	77 31 30 1 0
46	46 21 20 1 0	78	78 20 19 1 0
47	47 5 0	79	79 9 0
48	48 28 27 1 0	80	80 38 37 1 0
49	49 9 0	81	81 4 0
50	50 27 26 1 0	82	82 38 35 3 0
51	51 16 15 1 0	83	83 46 45 1 0
52	52 3 0	84	84 13 0
53	53 16 15 1 0	85	85 28 27 1 0
54	54 37 36 1 0	86	86 13 12 1 0
55	55 24 0	87	87 13 0
56	56 22 21 1 0	88	88 72 71 1 0
57	57 7 0	89	89 38 0
58	58 19 0	90	90 19 18 1 0
59	59 22 21 1 0	91	91 84 83 1 0
60	60 1 0	92	92 13 12 1 0
61	61 16 15 1 0	93	93 2 0
62	62 57 56 1 0	94	94 21 0
63	63 1 0	95	95 11 0
64	64 4 3 1 0	96	96 49 47 2 0
65	65 18 0	97	97 6 0
66	66 10 9 1 0	98	98 11 0
67	67 10 9 1 0	99	99 47 45 2 0
68	68 9 0	100	100 37 0
69	69 29 27 2 0	101	101 7 6 1 0
70	70 16 15 1 0	102	102 77 76 1 0
71	71 6 0	103	103 9 0
72	72 53 47 6 0	104	104 11 10 1 0
73	73 25 0	105	105 16 0
74	74 16 15 1 0	106	106 15 0
75	75 11 10 1 0	107	107 65 63 2 0
76	76 36 35 1 0	108	108 31 0

次数	本原多项式					次数	本原多项式				
109	109	7	6	1	0	139	139	8	5	3	0
110	110	13	12	1	0	140	140	29	0		
111	111	10	0			141	141	32	31	1	0
112	112	45	43	2	0	142	142	21	0		
113	113	9	0			143	143	21	20	1	0
114	114	82	81	1	0	144	144	70	69	1	0
115	115	15	14	1	0	145	145	52	0		
116	116	71	70	1	0	146	146	60	59	1	0
117	117	20	18	2	0	147	147	38	37	1	0
118	118	33	0			148	148	27	0		
119	119	8	0			149	149	110	109	1	0
120	120	118	111	7	0	150	150	53	0		
121	121	18	0			151	151	3	0		
122	122	60	59	1	0	152	152	66	65	1	0
123	123	2	0			153	153	1	0		
124	124	37	0			154	154	129	127	2	0
125	125	108	107	1	0	155	155	32	31	1	0
126	126	37	36	1	0	156	156	116	115	1	0
127	127	1	0			157	157	27	26	1	0
128	128	29	27	2	0	158	158	27	26	1	0
129	129	5	0			159	159	31	0		
130	130	3	0			160	160	19	18	1	0
131	131	48	47	1	0	161	161	18	0		
132	132	29	0			162	162	88	87	1	0
133	133	52	51	1	0	163	163	60	59	1	0
134	134	57	0			164	164	14	13	1	0
135	135	11	0			165	165	31	30	1	0
136	136	126	125	1	0	166	166	39	38	1	0
137	137	21	0			167	167	6	0		
138	138	8	7	1	0	168	168	17	15	2	0

附注：本表取自 Stahnke, W., Primitive Binary Polynomials, *Math. of Comp.* **16** (1962), 368—369.

参 考 书 目

[1] 万哲先、戴宗铎、刘木兰、冯绪宁，非线性移位寄存器，科学出版社，北京，1978.

[2] 王湘浩、谢邦杰，高等代数，第2版修订本，人民教育出版社，北京，1964.

[3] 王新梅，纠错码浅说，人民邮电出版社，北京，1976.

[4] 北京大学数学力学系几何与代数教研室代数小组，高等代数，人民教育出版社，北京，1978.

[5] 华罗庚，数论导引，科学出版社，北京，1975.

[6] 许以超，代数学引论，上海科学技术出版社，上海，1966.

[7] 张禾瑞，近世代数基础，人民教育出版社，北京，1978.

[8] 张禾瑞、郝炳新，高等代数，上下册，人民教育出版社，北京，1979.

[9] 张远达、熊全淹，线性代数，人民教育出版社，北京，1964.

[10] 库洛什(Курош, А. Г.)，一般代数学讲义(译自俄文)，上海科学技术出版社，上海，1964.

[11] 周伯埙，高等代数，人民教育出版社，北京，1978.

[12] 林(S. Lin)，纠错编码入门(译自英文)，人民邮电出版社，北京，1976.

[13] 范德瓦尔登(van der Waerden, B. L.)，代数学(译自德文第四版)，卷 I，和卷 II，科学出版社，北京，1978.

[14] 贾柯勃逊(Jacobson, N.)，抽象代数学(译自英文)，卷 I (基本概念)和卷 II(线性代数)，科学出版社，北京，1960.

[15] 熊全淹，近世代数学，第二版，上海科学技术出版社，上海，1978.

[16] Albert, A. A., Fundamental Concepts of Higher Algebra. The University of Chicago Press, Chicago, U. S. A., 1956.

[17] Berlekamp, E. R., Algebraic Coding Theory, McGraw-Hill Book Company, New York, U. S. A., 1968.

[18] Blake I. F. and Mullin, R. C., The Mathematical Theory of Coding, Academic Press, 1975.

[19] Gill, A., Linear Soquential Circuits, McGraw-Hill, 1966.

[20] Golomb, S. W. (edited by), Digital Communications with Space Applications, Prentice-Hall, Englewood Cliffs, New Jersey, U. S. A., 1964.

[21] Golomb, S., Shift Register Sequences, Holden-Day, San Francisco, U. S. A., 1967.

[22] Hall, M., Combinatorial Theory, Blaisdell Publishing Company, Waltham, Massachusett, U. S. A., 1967.

[23] Hoffmann de Visme, G., Binary Sequences, The English Universities Press, London, United Kingdom, 1971.

[24] Jacobson, N., Lectures in Abstract Algebras, Volume III—Theory of Fields and Galois Theory, D. Van Nostrand Company, Inc., Princeton, New Jersey, U. S. A., 1964.

[25] Kautz, W. H. (edited by), Linear Sequential Switching Circuits, Holden-Day, San Francisco, U. S. A., 1965.

[26] Mac Williams, F. J. and Sloane, N. J. A., The Theory of Error-correcting Codes, zpts., North-Holland Publishing Company, Amsterdam, 1977.

[27] Peterson, W. W. and Weldon, E. J. Jr., Error-Correcting Codes, 2nd ed., M. I. T. Press, Cambridge, Massachusett, U. S. A., 1971.

[28] Van Lint, J. H. Coding Theory, Springer-Verlag. 1971.

名 词 索 引

二 划

三 划

四 划

五 划

六 划

七 划

八 划